DISCIPLINE: Minimum Desktop Hardware

Discipline Roadmap for: Desktop

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Dell Pentium IV Compaq Gateway Macintosh HP Intel **Compatible** Processor Apple MacIntosh	Pentium IV compatible	Market Watch

Shared	Agency
	✓

Retirement Targets

Lower than Pentium III

Mainstream Platforms (must be supported)

Pentium IV or Higher

Containment Targets

Emerging Platforms

MacIntosh

Implications and Dependencies

– Cannot upgrade O/S and certain application software until hardware is upgraded/replaced

Roadmap Notes – State Procurement Office to establish best buying practices and vendors for PC purchases.

Minimum PC Configuration Reviewed Annually after Adoption by AOC

DISCIPLINE: Minimum Desktop Hardware (Cont’d)

Discipline Roadmap for: Desktop

- **Discipline Boundaries:**
  - These are required minima.
- **Discipline Minimum Standards:**

  Processor: Pentium IV Compatible   Memory: 512 MB RAM

  Storage: 80GB+ EIDE, CD/DVD±-R
- **Migration Considerations:**
  - Organizations should proactively migrate off of desktop hardware less than Pentium IV based on depreciation schedules and budget.
  - Hardware must be sufficient to support O/S and O/S application must be certified by vendor to be supported.
- **Exception Considerations:**
  - Specialized applications with specialized platforms need to be reviewed by AOC.
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - March 24, 2004
- **Date Last Updated:**
  - April 22, 2006
- **Next Review Date:**
  - April 2007

DISCIPLINE: Minimum Laptop Hardware

Discipline Roadmap for: Laptop

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Compaq Notepads Notebook- Dell Dell CPI Dell Inspiron Gateway Hitachi IBM ThinkPad Apple MacIntosh	Pentium IV compatible	Market Watch

Shared	Agency
	✓

Retirement Targets

Lower than Pentium III

Mainstream Platforms (must be supported)

Pentium IV or higher

Containment Targets

Emerging Platforms

MacIntosh

Implications and Dependencies

Cannot upgrade O/S and certain application software until hardware is upgraded/replaced.

Roadmap Notes –

Minimum PC configuration reviewed annually after adoption by AOC

DISCIPLINE: Minimum Laptop Hardware

Discipline Roadmap for: Laptop

- **Discipline Boundaries:**
  - ❑ All business laptops, does not include laptops used for special purposes. These are required minimums.
- **Discipline Minimum Standards:**

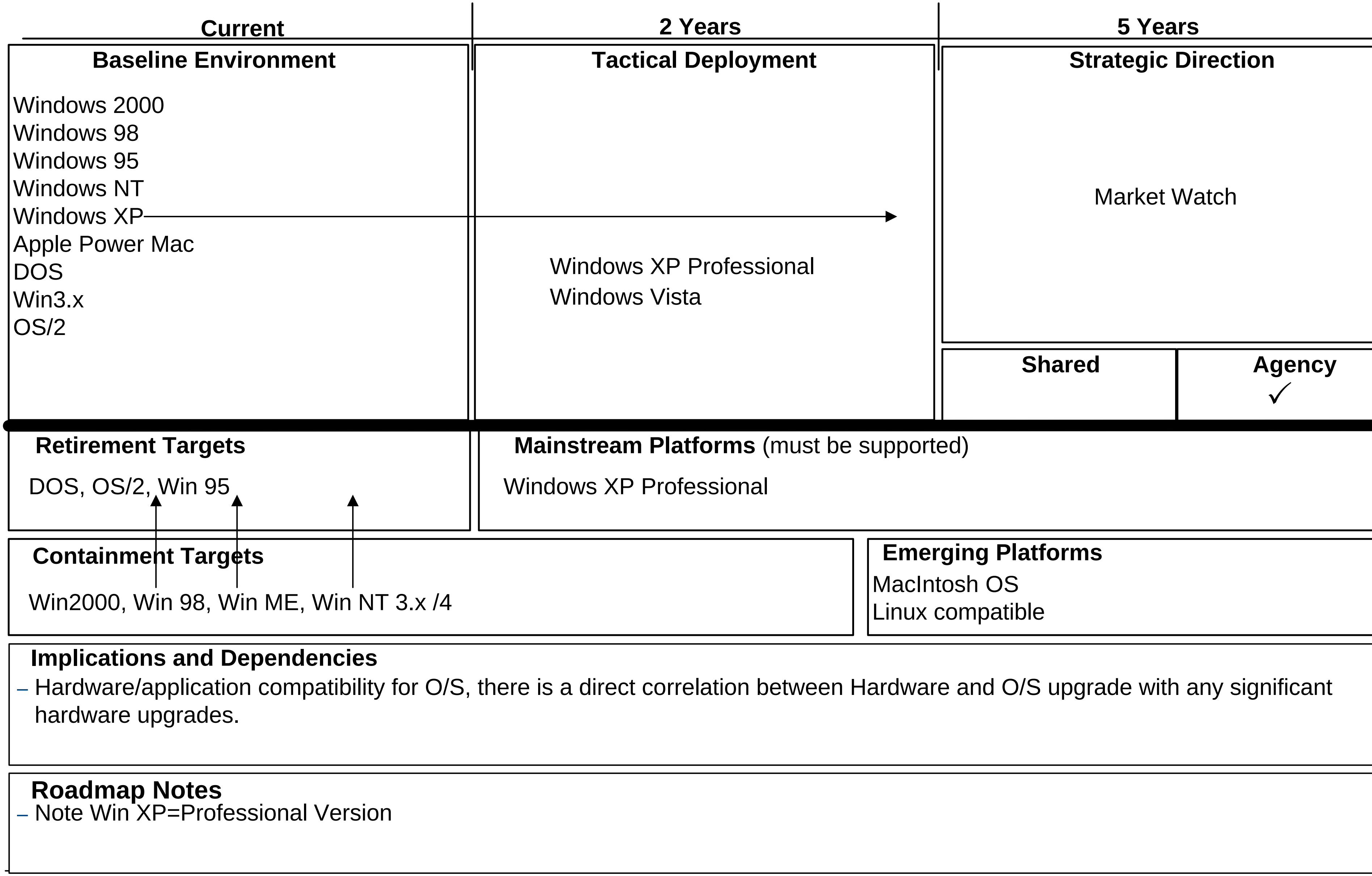
Processor: Pentium IV Compatible   Memory: 512MB

Storage: 40GB HD; CD-RW

- **Migration Considerations:**
  - ❑ Hardware must be sufficient to support O/S and O/S applications must be certified by vendor to be supported.
- **Exception Considerations:**
  - ❑ Special purpose laptops, e.g., machines used for maintenance or security or other special/unique application support do not fall under this standard and do not require an approved exception. If questions arise regarding whether a laptop falls under this exception, please contact the CIO Architecture Support Group.
- **Miscellaneous Notes:**
  - ❑ Consider wireless hardware impact and security.
- **Established Date**
  - ❑ March 24, 2004
- **Date Last Updated:**
  - ❑ April 22, 2006
- **Next Review Date:**
  - ❑ April 2007

DISCIPLINE: Client Operating Systems

Discipline Roadmap for: Client OS



Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Windows 2000 Windows 98 Windows 95 Windows NT Windows XP → Apple Power Mac DOS Win3.x OS/2	Windows XP Professional Windows Vista	Market Watch

Shared	Agency
	✓

Retirement Targets

DOS, OS/2, Win 95

Mainstream Platforms (must be supported)

Windows XP Professional

Containment Targets

Win2000, Win 98, Win ME, Win NT 3.x /4

Emerging Platforms

MacIntosh OS
Linux compatible

Implications and Dependencies

– Hardware/application compatibility for O/S, there is a direct correlation between Hardware and O/S upgrade with any significant hardware upgrades.

Roadmap Notes

– Note Win XP=Professional Version

DISCIPLINE: Client Operating Systems (Cont'd)

Discipline Roadmap for: Client OS

- **Discipline Boundaries:**
  - All Desktop PC's that are used in routine business operations. Does not include specialized desktops.
- **Discipline Standards:**
  - Intel Compatible
- **Migration Considerations:**
  - Expected timelines for support discontinuity and budget constraints.
- **Exception Considerations:**
  - Exceptions will be driven by special applications.
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - November 19, 2003
- **Date Last Updated:**
  - April 22, 2006
- **Next Review Date:**
  - April 2007

DISCIPLINE: Collaborative File Formats

Discipline Roadmap for: Collaborative File Formats

Current	2 Years	5 Years
Baseline Environment Hundreds of formats, including: Word Processing: RTF, DOC (Word), DOC (WordPerfect), WRI Spreadsheet: XLS, WKS, WBx Database: DBF, DB , MDB Presentation: PRS, PPT Data Exchange: TXT, CSV Graphics: TIFF, JPG, GIF, BMP, WMF, PCX, CDR, PSD, PNG, PDF, EPS, AI, DWG, DXF, ART Sound: WAV, MP3, MIDI, CDA Video: AVI, MPEG, DV, WMV, RM, ASF	**Tactical Deployment** Word Processing: DOC (Word), RTF Spreadsheet: XLS Database: MDB Presentation: PPT Data Exchange: TXT, CSV, XML Graphics: TIFF, JPG Sound: WAV, MP3 Video: AVI, MPEG, WMV, SWF Forms/Document Display: PDF, XML	**Strategic Direction** Market Watch

Shared	Agency
	✓

Retirement Targets

File formats used/generated only by software targeted for retirement

Mainstream Platforms

File formats generated by supported software packages (e.g., Office XP)

Containment Targets

File formats generated/used only by software currently under containment

Emerging Platforms

Implications and Dependencies

Availability of programming support may dictate moving some formats from “containment” to “retirement” status.

Simplifying file formats is critical to reducing training and support requirements and enhancing workgroup and enterprise productivity

Roadmap Notes –

Standard to be reviewed annually after adoption by AOC.

DISCIPLINE: Collaborative File Formats

Discipline Roadmap for: Collaborative File Formats

- **Discipline Boundaries:**
  - File formats for dissemination or modification of information with internal and external users.
- **Migration Considerations:**
  - Documents/spreadsheets/etc. with extensive internal programming may require reprogramming as part of the migration process.
  - Appropriate “viewers” may need to be made available via internal and external web sites for those without software to read standard file formats in native mode.
- **Exception Considerations:**
  - Some activities may require non-standard formats to accommodate special-purpose needs (e.g., architectural drawings, mapping functions).
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - April 28, 2004
- **Date Last Updated:**
  - April 22, 2006
- **Next Review Date:**
  - April 2007

DISCIPLINE: Dumb Terminals

Discipline Roadmap for: Dumb Terminals

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Mainframe 3270 DEC VT 220, 320, 420 MTX (Memorex Telex) Unix VT100 TN 3270 (freeware) → PC Emulators	→	Eliminate

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

TN 3270

Containment Targets

Mainframe 3270; DEC VT 220, 320, 420; Unix VT100; MTX

Emerging Platforms

Implications and Dependencies-

All State facilities need to be IP network connected.

Roadmap Notes

DISCIPLINE: Dumb Terminals (Cont'd)

Discipline Roadmap for: Dumb Terminals

- **Discipline Boundaries:**
  - Non PC based end user data entry and display devices
- **Discipline Standards:**
  - TN 3270
- **Migration Considerations:**
- **Exception Considerations:**
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - March 24, 2004
- **Date Last Updated:**
  - April 22, 2006
- **Next Review Date:**
  - April 2007

DISCIPLINE: Personal Digital Assistant Operating Systems

Discipline Roadmap for: Operating System for PDAs

DOMAIN: PRESENTATION SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Palm OS → Windows for Pocket PC → Rim Blackberry →	→	Market watch

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms

Palm OS, Windows for Pocket PC, Rim Blackberry

Containment Targets

Emerging Platforms

Market watch

Implications and Dependencies

PDA Operating system must exchange files with standard desktop operating system.

Roadmap Notes

Need research into who and where personal devices are being used.

DISCIPLINE: Personal Digital Assistant Operating Systems

Discipline Roadmap for: Operating System for PDAs

- **Discipline Boundaries:**
  - Two basic operating systems dominate the handheld personal digital assistants (PDAs) uses in South Carolina government; Palm OS and Windows for Pocket PC.
  - Various local requirements for feature, service, and compatibility to outside partners lead to this need for flexibility in platform choice. One such example is the use of mobile telephony incorporated in PDA devices. Not all voice carriers recognize and utilize all PDA devices that have such capabilities. Collaboration and information sharing between agency and private sector parties is yet another.
- **Discipline Standards:**
  - While the Windows for Pocket PC user and developer market continues to grow rapidly, there remains justification and need for the use of industry standard Palm OS products in some areas. Therefore, it is the position of the Presentations Sub-domain committee that no one PDA platform be emphasized across the board at the present time.
  - However, this fast and ever-changing technology should be monitored and updated as trends, needs, and advancements take place.
- **Migration Considerations:**
  - This standard should not require any migrations except release to release as dictated by the vendors and devices.
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - April 28, 2004
- **Date Last Updated:**
  - April 27, 2005
- **Next Review Date:**
  - April 2006

DISCIPLINE: Desktop Productivity Tools

Discipline Roadmap for: Desktop Productivity Tools

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Office 97 Standard/Professional Office 2000 Standard/Professional Office XP Standard/Professional WordPerfect Office Lotus SmartSuite Star Office Legacy Word Processing/ Spreadsheet/Presentation Packages	Office XP Standard/Professional Office 2003 Standard/Professional Open Office 2.0	Market Watch

Shared	Agency
	✓

Retirement Targets

Legacy Packages
Suites Incompatible with Standard OS

Mainstream Platforms

Office XP, Office 2003, Open Office 2.0

Containment Targets

WordPerfect Office/Lotus SmartSuite/Star Office/Office 2000 and earlier

Emerging Platforms

Office Services

Implications and Dependencies

Future availability of vendor support may dictate moving some packages from “containment” to “retirement” status.

Backward compatibility and ability to read older formats are critical.

Roadmap Notes –

Standard to be reviewed annually after adoption by AOC.

DISCIPLINE: Desktop Productivity Tools

Discipline Roadmap for: Desktop Productivity Tools

- **Discipline Boundaries:**
  - ❑ Office productivity suites for general use.
- **Migration Considerations:**
  - ❑ Hardware and operating system may need to be upgraded to standards before migration.
  - ❑ Documents/spreadsheets/etc. with extensive internal programming may require revision as part of the migration process.
- **Exception Considerations:**
  - ❑ Users heavily involved with programming or end-user support may require Developer versions of standard suites and/or non-supported packages.
- **Miscellaneous Notes:**
  - ❑ None
- **Established Date**
  - ❑ April 28, 2004
- **Date Last Updated:**
  - ❑ April 22, 2006
- **Next Review Date:**
  - ❑ April 2007

DISCIPLINE: Web Accessibility

Discipline Roadmap for: Web Accessibility

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Initial efforts to date have focused on on-going: •Research •Education •Training •Collaboration •Agency Partnerships	Minimal Requirements: Section 508 Standards Best practices: W3C-WAI Guidelines	The standards and guidelines should be reviewed annually to ensure agency Web sites are in compliance with the latest revisions to state and federal laws,

Shared	Agency
✓	

Retirement Targets

Not Applicable

Mainstream Platforms

Not Applicable

Containment Targets

Not Applicable

Emerging Platforms

Not Applicable

Implications and Dependencies

South Carolina state government Web sites shall be designed to be accessible, so that people with disabilities have access to online information, data, and services comparable to that accorded individuals who do not have disabilities.

Roadmap Notes –

For more details and information, please reference the Web Accessibility Policy listed on the SC Enterprise Architecture website under ‘Information’ & ‘Documents/Forms’ at www.cio.sc.gov

DISCIPLINE: Web Accessibility

Discipline Roadmap for: Web Accessibility

- **Discipline Boundaries:**
  - This standard applies to internal and external accessible websites and applications.
- **Migration Considerations:**
  - As soon as possible, each agency should conduct a self-assessment of its web presence, develop and maintain a written plan.
  - Achieve minimum requirements (Section 508 standards) by July 2006. Best practices (W3C-WAI Guidelines) are encouraged.
- **Exception Considerations:**
  - It is not required that all pages be retrofitted. Excluded are: legacy pages that do not require content update and instances in which undue burden can be proven.
  - Each agency shall establish a mechanism for collecting and responding within a reasonable length of time to comments, complaints and suggestions about accessibility of it Web presence.
- **Miscellaneous Notes:**
  - To provide assistance to agencies, the South Carolina Web Accessibility Workgroup of the Assistive Technology Advisory Committee (ATAC) shall create an official State of South Carolina Accessibility Web site (www.access-sc.org) to provide a list of resources and training opportunities.
- **Established Date:**
  - June 23, 2004
- **Date Last Updated:**
  - April 22, 2006
- **Next Review Date:**
  - April 2007

DISCIPLINE: Assistive Technology

Discipline Roadmap for: Assistive Technology

Current	2 Years	5 Years	
Baseline Environment	**Tactical Deployment**	**Strategic Direction**	
Baseline environment was not collected.	Use ‘Best Practices’ to select the technologies that works best for the person with the disability.		
		Shared	**Agency** ✓

Retirement Targets

Not Applicable

Mainstream Platforms

Not Applicable

Containment Targets

Not Applicable

Emerging Platforms

Implications and Dependencies

Use latest software version and install updates as available. The end-user, the person with the disability, should play a key role in determining what works best.

Roadmap Notes

DISCIPLINE: Assistive Technology

Discipline Roadmap for: Assistive Technology

- **Discipline Boundaries:**
  - ❑ General desktop office automation tools.
- **Discipline Standards:**
  - ❑ Please review 'Best Practices' on the SCEA website.
- **Migration Considerations:**
  - ❑ Before ordering additional software, review built-in accessibility options.
- **Exception Considerations:**
  - ❑ None
- **Miscellaneous Notes:**
  - ❑ The Presentation Services Domain Subcommittee worked with the South Carolina Assistive Technology Advisory Committee to determine 'Best Practices' for this technology. 'Best Practices' is available on the SCEA website or can be obtained from the Architecture Support Group at the CIO.
- **Established:**
  - ❑ September 2004
- **Date Last Updated:**
  - ❑ April 22, 2006
- **Next Review Date:**
  - ❑ April 2007

Web Site Accessibility Policy and Transition Plan for the State of South Carolina

I. Policy

The State of South Carolina is committed to providing accessibility to state government Internet-based resources.

South Carolina state government Web sites shall be designed to be accessible, so that people with disabilities have access to online information, data, and services comparable to that accorded individuals who do not have disabilities.

II. Guidelines

Following the Guidelines (described in Parts A and B below) and the Transition Plan (outlined in Part III) will assist a state agency in ensuring that its Web presence is accessible to the widest possible range of users.

Implementation of the Minimal Requirements in Part A satisfies basic accessibility requirements for state government Web pages. In addition, agencies are encouraged to go beyond the minimum in making Web pages accessible by following the Best Practices in Part B.

A. Minimal Requirements

The State of South Carolina shall follow the standards established under Section 508 of the Rehabilitation Act of 1973, amended 1998 by the Work Force Investment Act (Section 1194.22 and its subsequent amendments), as its minimal requirements for Web accessibility. [See Appendix 1.]

B. Best Practices

It is recommended that agencies also follow the Web Content Accessibility Guidelines established by the World Wide Web Consortium‘s Web Accessibility Initiative (W3C-WAI) that are not addressed in Section 508. [See Appendix 2.]

III. Transition Plan

A. Self-Assessment

Each agency shall review the current status of accessibility for its Web presence**.**

This review does not require an agency to evaluate each page of a site, but instead requires the agency to appraise the overall accessibility of its Web presence.

As a starting point, it is suggested that each agency evaluate the accessibility of the most frequently visited pages and a random sampling of other pages.

B. Plan

Each agency shall develop, keep on file, and implement a written plan for making its Internet Web presence accessible as well as a plan for making its Intranet Web presence accessible. The planning documents shall include provisions for necessary staff training.

Each agency head shall appoint an individual with sufficient authority and resources to be responsible for overseeing the implementation of the agency's plans.

C. Deadline

The deadline for achieving accessibility on Internet sites, as outlined in Section D, shall be no later than two years from the passage of the policy by the Architecture Oversight Committee (AOC) plus a review period of 21 days from the posting of this policy on the AOC Web site. (The deadline for Internet site compliance is July 21, 2006.)

The deadline for achieving Intranet site accessibility, as outlined in Section D, shall be no later than 2 years after the Internet site deadline. (The deadline for compliance is July 21, 2008.)

D. Order of Implementation

Each agency shall implement Web site accessibility in the following order:

1. Main entry pages, home pages, top-level pages, most frequently visited pages, and pages that provide mission-critical agency services.
2. Front-end user interfaces that provide access to agency applications.
3. All new pages and interfaces created after the deadline.
4. Legacy pages and interfaces updated after the deadline.

E. Exceptions

It is not required that all pages be retrofitted.

Expressly excluded are:

1. Legacy pages that do not require content updates.
2. Legacy front-end user interfaces that do not require content updates.
3. Instances in which undue burden can be proven.

However, if an individual with a disability requests specific information published in an inaccessible section of a Web site, each agency shall, within a reasonable length of time, provide the requested information or data in a format accessible to that individual or by an alternative means of access that allows the individual to use the information and data.

F. Feedback Mechanism

Each agency shall establish a mechanism for collecting and responding within a reasonable length of time to comments, complaints, and suggestions about accessibility of its Web presence.

G. Resources

Recognizing that agencies may need assistance in carrying out this policy and plan, the South Carolina Web Accessibility Workgroup of the Assistive Technology Advisory Committee (ATAC) shall create an official State of South Carolina Accessibility Web site to provide a list of resources and training opportunities, and recommended topics for training.

IV. Definitions

A. Access Board

The Access Board is an independent Federal agency devoted to accessibility for people with disabilities. Under Section 508 of the Rehabilitation Act Amendments, the Access Board published standards for electronic and information technology, including Web access.

B. Architecture Oversight Committee (AOC)

The charge of the Architecture Oversight Committee (AOC) is to advise the State Budget and Control Board's Division of the State Chief Information Officer on how the State might best use technology to become a recognized leader in delivering cost effective services desired by citizens, businesses, and government organizations, while maximizing constituent participation in the governmental process.

C. Assistive Technology Advisory Committee (ATAC)

The role of the South Carolina Assistive Technology Advisory Committee is to assist State government in meeting its obligation to provide access to government information for all South Carolinians.

D. Agency

See "State Agency."

E. Disability

The term "disability" with respect to an individual as defined by the Americans with Disabilities Act (ADA) means:

1. A physical or mental impairment that substantially limits one or more of the major life activities of such individual. Major life activities include: seeing, hearing, speaking, walking, breathing, performing manual tasks, learning, caring for oneself, and working;
2. A record of such an impairment; or
3. Being regarded as having such an impairment.

If an individual meets any one of these three tests, he or she is considered to be an individual with a disability.

F. Legacy Pages

Web pages created prior to the effective date of this policy.

G. State Agency

Each department, office, board, bureau, commission, and other unit of the executive, legislative, and judicial branches of state government, including public four- and two-year colleges and universities.

H. Undue Burden

Undue burden means significant difficulty or expense. In determining whether an action would result in an undue burden, an agency shall consider all agency resources available to the agency or components for which the product is being developed, procured, maintained, or used.

I. Web Presence

While Web presence is often used as a synonym for the term Web site, Web presence further expresses the idea of a virtual presentation in "cyberspace."

Web presence includes anything associated with an agency’s official Web site(s), whether reached through the Internet or an intranet, extranet, or courseware.

J. Web Accessibility Initiative (WAI)

The WAI, in coordination with organizations around the world, pursues accessibility of the Web through five primary areas of work: technology, guidelines, tools, education and outreach, and research and development. This initiative is a subset of W3C.

K. World Wide Web Consortium (W3C)

The W3C is an international industry consortium of approximately 500 organizations. W3C was created to establish Web standards and lead the Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability.

Appendix 1 – Section 508 Standards for Web Accessibility

Section 508 of the Rehabilitation Act of 1973, amended 1998 by the Work Force Investment Act sets standards for hardware, software, and Web accessibility. The Section 508 Web accessibility standards are listed below.

§ 1194.22 Web-based intranet and internet information and applications.
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.
(d) Documents shall be organized so they are readable without requiring an associated style sheet.
(e) Redundant text links shall be provided for each active region of a server-side image map.
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.
(g) Row and column headers shall be identified for data tables.
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.
(i) Frames shall be titled with text that facilitates frame identification and navigation.
(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).
(n) When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.
(o) A method shall be provided that permits users to skip repetitive navigation links.
(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

Note to §1194.22: 1. The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5, 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium:

Section 1194.22 Paragraph	WCAG 1.0 Checkpoint
(a)	1.1
(b)	1.4
(c)	2.1
(d)	6.1
(e)	1.2
(f)	9.1
(g)	5.1
(h)	5.2
(i)	12.1
(j)	7.1
(k)	11.4

2. Paragraphs (l), (m), (n), (o), and (p) of this section are different from WCAG 1.0. Web pages that conform to WCAG 1.0, level A (i.e., all priority 1 checkpoints) must also meet paragraphs (l), (m), (n), (o), and (p) of this section to comply with this section. WCAG 1.0 is available at http://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505.

Appendix 2 – W3C-WAI Web Accessibility Guidelines

The World Wide Web Consortium's Web Accessibility Initiative (W3C-WAI) developed guidelines for Web accessibility. The current guidelines are the Web Content Accessibility Guidelines 1.0.

A new Working Draft of Web Content Accessibility Guidelines 2.0 has been developed and is under review.

Assistive Technology – Best Practices

The specific need for assistive technology is unique to the individual. "Trial-and-error may be required to find a set of appropriate tools and techniques. The end user—the person with a disability—should play a key role in determining what works best" (Burgstahler & Comden, 2002).

Disability	AT/Accommodations	Products/Vendors	Comments
Vision Impairment	High Contrast	MS Windows Accessibility Options	Allows user to change colors and fonts for easy reading (start-settings-control panel-accessibility options).
	Cursor Options	MS Windows Accessibility Options	Changes the speed that the cursor blinks and the width of the cursor (start-settings-control panel-accessibility options).
	Toggle Keys	MS Windows Accessibility Options	Produces a tone when pressing CAPS LOCK, NUM LOCK, SCROLL LOCK (start-settings-control panel-accessibility options).
	Narrator	MS Windows Accessibility Options (MS Windows 2000 or higher)	Reads aloud menu commands, dialog box and more (start-programs-accessories-accessibility).
	Magnifier	MS Windows Accessibility Options (MS Windows 98 or higher)	Provides variable magnification settings and allows user to invert color (start-programs-accessories-accessibility).
	Large Screen Fonts	MS Windows Display Settings	Provides large fonts on the screen (start-control panel-display-appearance).
Vision Impairment (continued)	Large Monitor (19" or larger)	Retail store (Best Buy, Circuit City, etc.) or designated procurement manufacturer	

	Large Print Keyboard Key Labels	Zoom Caps/maxiaids.com, donjohnston.com Large Print Keytop Labels/infogrip.com	Labels for top of keys on keyboard. Includes all alpha-numeric characters. Available in various color combinations.
	Glare Guard	Retail store (Office Max, Staples, etc.) or designated procurement manufacturer	A screen placed in front of a computer display screen which reduces glare and helps the user avoid eyestrain and enhances readability.
	Large Cursor	Biggy/rjcooper.com	Provides selection of ultra-visible cursors that work within any software.
	Screen Magnification Software	Zoom Text Xtra Level 1/aisquared.com, infogrip.com MAGic® Screen Magnifier-No Speech/ infogrip.com, freedomscientific.com BigShot/aisquared.com	Full and partial screen enlargement.
	Screen Magnification Software with Screen Reader	Zoom Text Xtra Level 2/aisquared.com, infogrip.com	Full and partial screen enlargement with screen reader.
		MAGic® Screen Magnifier-With Speech/ infogrip.com	Limited screen reader capability. Compatible with screen reader software (i.e. JAWS® for Windows)
	High Contrast Colors	MS Windows Display Settings	Allows selection of high contrast colors to enhance screen readability (start-control panel-display-appearance).
	Colors Compatible for People with Color Blindness	MS Windows Display Settings	Allows selection of various colors to enhance screen readability (start-control panel-display-appearance).
Blindness	Screen Reader	JAWS® for Windows/ GSTSdesigns.com, freedomscientific.com, maxiaids.com	Makes documents, internet and commands audible. JAWS® has output to refreshable Braille displays.

		WYNN™/freedomscientific.com, donjohnston.com, Key Technologies, Inc.	
	OCR (Scanner)	Retail store (Office Max, Staples, etc.) or designated procurement manufacturer	Reads text from paper and translates into a computer document.
	Braille Printer	Braille Blazer/freedomscientific.com	Prints Braille on many sizes of Braille paper, plastic labels and even index cards. Internal speech synthesizer that allows quick and simple configuration.
	Braille Keytops for Keyboard	Braille Keytop Labels/maxiaids.com	Provides Braille stickers for application to surface of keyboard keys.
	Headphones	Retail store (Office Max, Staples, etc.) or designated procurement manufacturer	Allows use of auditory features without disturbing others nearby.
Deafness/ Hearing Impairment	Sound Sentry	MS Windows Accessibility Options	Provides visual warnings when your system makes a sound (start-settings-control panel-accessibility options).
	Show Sounds	MS Windows Accessibility Options	Allows programs to show captions for the speech and sounds they make (start-settings-control panel-accessibility options).
Deafblind	Refreshable Braille Display	Focus Braille Displays/freedomscientific.com, ALVA Satellite Braille Displays/alvabraille.com	Displays Braille characters by means of raising the dots through holes in a flat surface.
Mobility Impairment	Computer Location Accessible for Wheelchairs		Accommodates a wheelchair for access to the monitor, keyboard and mouse.

	Adjustable Computer Workstation	Accessible Computer Station/ dbhattachments.com	Accommodates a wheelchair for access to the monitor, keyboard and mouse.
	Wireless Keyboard and Mouse	Logitech Cordless/logitech.com Retail store (Best Buy, Circuit City, etc.) or designated procurement manufacturer.	Allows computer access from a distance.
Manual Dexterity Impairment	Adjustable Computer Workstation	Accessible Computer Station/dbhattachments.com	Accommodates the wheelchair for access to the monitor, keyboard and mouse.
	Ergonomic Chair	Retail store (Office Max, Staples, etc.) or designated procurement manufacturer	Facilitates correct positioning to reduce fatigue and facilitate access.
	Foot Rest	Adjustable Foot Rest or Footrester/ infogrip.com	Redistributes body weight to decrease strain and fatigue on legs, back and neck.
	Keyguard for Keyboard	turningpointtechnology.com, techable.org	Maximizes physical access to accurately target keys on the keyboard. Makes customized keyguards.
	Trackball Mouse	Retail store (Best Buy, Circuit City, etc.) or designated procurement manufacturer. Penny & Giles Roller Plus Trackball/ GSTSdesigns.com, infogrip.com, donjohnston.com, dunamisinc.com, Key Technologies, Inc.	Includes buttons that support right and left click, double click, drag lock, horizontal and vertical lock, and cursor speed control.
	Orbit Optical Trackball Mouse	Kensington Orbit Optical Trackball mouse/kensington.com	Allows the user to control the cursor with a simple touch of the finger.
Manual Dexterity Impairment	Joystick Mouse Emulator	Retail store (Best Buy, Circuit City, etc.) or designated procurement manufacturer. Penny & Giles Roller Plus Joystick/	Includes buttons that support right and left click, double click, drag lock, horizontal and vertical lock, and cursor speed control.

(continued)		GSTSdesigns.com, infogrip.com, donjohnston.com, dunamisinc.com, Key Technologies, Inc.	Roller Plus products include a key guard to help users isolate the buttons.
	Alternative Keyboard	Expanded keyboard with keyguard: Big Keys/bigkeys.com, dunamisinc.com, Key Technologies, Inc. Intellikeys ® /intellitools.com, dunamisinc.com, Key Technologies, Inc.	Includes simplified keyboard with large keys. QWERTY or alphabetized key arrangements are available.
		Ergonomic keyboards: Retail store (Best Buy, Circuit City, etc.), designated procurement manufacturer, or infogrip.com, maltron.com	Helps prevent cumulative trauma disorders. Some models have flexibility to accommodate specific disabilities.
		Mini keyboards: tashinc.com, GSTSdesigns.com	Allows access with minimal movement. Can control both keyboard and mouse functions. Can be used with mousestick or head pointer.
	One-Handed Typing	Half-Qwerty Typing Software/half-qwerty.com	Facilitates the transfer of two-handed typing skill to the one-handed condition. Typing is performed on a standard keyboard.
		Maltron Single-Handed Keyboard/maltron.com Bat Keyboard/infogrip.com	Replicates all the functions of a full-size keyboard, but with greater efficiency and convenience. Keyboard arrangement minimizes finger movement.
	Arm and Wrist Supports	Articulating Arm Supports/ergopages Ergorest Arm Supports/infogrip.com	Provides comfortable arm, shoulder and neck support with unrestricted motion. Muscle tension in the neck and shoulders can be significantly reduced.
Manual Dexterity Impairment	Touch Monitor	Key Technologies, Inc., Keytec, Inc./magictouch.com	Allows the user to make selections, move objects, and pull down menus with the touch of a finger on the monitor screen.

(continued)	Touch Window	infogrip.com, dunamisinc.com	Attaches to a computer monitor. Allows the user to make selections, move objects, pull down menus with the touch of a finger.
	E Z Keys	Key Technologies, Inc., Words +/words-plus.com	Provides text-based voice output with word prediction. Stores user-made phrases. All access modes.
	Sticky Keys	MS Windows Accessibility Options	Allows one-handed typists to use SHIFT, CTL, ALT keys (start-settings-control panel-accessibility options).
	Filter Keys	MS Windows Accessibility Options	Ignores brief or repeated key strokes or slows the repeat rate (start-settings-control panel-accessibility options).
	Mouse Keys	MS Windows Accessibility Options	Uses the numeric keypad to control the movement of the cursor (start-settings-control panel-accessibility options).
	Word Prediction Software	Co:Writer®/donjohnston.com E Z Keys™ for Windows/ Key Technologies, Inc., Words +/words-plus.com	Predicts the word you are typing and the next word based on word frequency and context. May also include features such as spell check, speech synthesis, and hotkeys for frequently used words.
	Switches	Tash/tashinc.com, Ablenet/ablenet.com, GSTSdesigns.com, Key Technologies, Inc.	Allows user to access a computer with a push of various body parts against a switch surface.
Lack of Manual Dexterity	Head/Chin Pointer	zygo-usa.com, allegromedical.com	Attaches pointer to head with straps.
	Electronic Pointing Device	Head Mouse® Extreme/orin.com	

Lack of Manual Dexterity	Mouthstick Typing Aid or Typing Pointer Foot Mouse Voice Input Software On-Screen Keyboard Microphone	mouthstick.net Typing Aid/westons.com, activeforever.com, secureic.getontech.com No Hands Mouse/abilityhub.com, I/O Foot Mouse/iotest.net Dragon Naturally Speaking/ scansoft.com, GSTSdesigns.com, maxiaids.com MS Windows Accessibility Options (MS Windows 2000 or higher) Softtype/orin.com, GSTSdesigns.com Parrott Talk Pro USB/GSTSdesigns.com	Replaces a standard computer mouse for people who cannot use their hands. The wireless sensing technology employs infrared light to track the user's head movements. Allows user to type or manipulate items by using a stick controlled by mouth. Straps to hand. Extending wand strikes keys. Eliminates wasteful, repetitive "keyboard-to-mouse" hand movements. Turns speech into text. The user can create documents, enter data, launch applications, send e-mail, complete forms, and browse the Web. Various editions available based on profession and needs. Training required. Allows users to mouse click, hover, or use joystick to select key (start - programs - accessories - accessibility). Integrates AutoClick™ and Dragger™ for performing clicking functions by dwell selection, multiple keyboard layouts, word completion with customizable word list, and excellent companion for HeadMouse® or other mouse emulators. Provides high quality voice input for maximum accuracy with use of voice-to-text

(continued)			software (i.e. Dragon Naturally Speaking).
Vision and Manual Dexterity Impairment	Middle Software	Jaw Bone/GSTSdesigns.com, maxiaids.com, synapseadaptive.com	Allows Dragon Naturally Speaking and Jaws® to work together.
	Screen Magnification Software with Screen Reader	Zoom Text Xtra Level 2/aisquared.com, infogrip.com	Provides full and partial screen enlargement with screen reader.
Cognitive impairment	Text to Voice Software	Wynn™/freedomscientific.com, Key Technologies, Inc. Kurzweil/kurzweiledu.com	Adds auditory component to written material to facilitate understanding.
	Language at the Third Grade Level	Microsoft Word Options	Includes a Flesch-Kincaid readability grade level, which is shown in the summary after spell check is completed (In Microsoft Word document: tools-options-spelling/grammar-check “readability statistics”).

- Before ordering additional software, review built-in accessibility options. See Accessibility Wizard (MS Windows 2000 or higher: start - programs - accessories - accessibility).
- Use the latest software version and install updates as available.
- Software that includes text to speech features (ex.: Zoom Text 2) may not work while JAWS® is active.
- Dragon Naturally Speaking dominates the sound card for its sole use; therefore, the sound feature may not be available in other software programs.

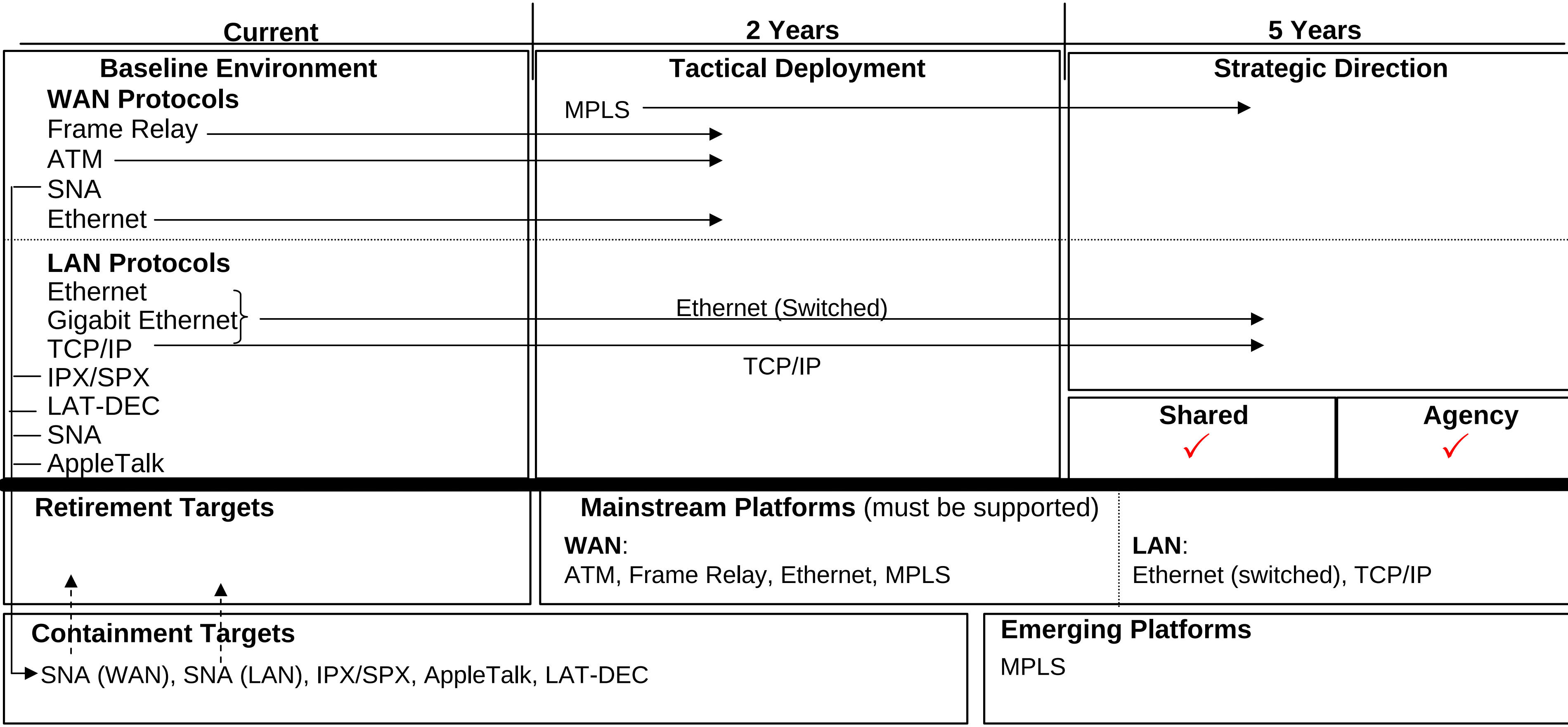
Reference

Burgstahler, S. & Comden, D. (2002). Working together: Computer technology and people with mobility & sensory impairments. Exceptional Parent Magazine, *p. 36.*

For further information, or consultation, call the South Carolina Assistive Technology Project, Evelyn Evans, Director, (803) 935-5263, www.sc.edu/scatp.

DISCIPLINE: WAN/LAN Protocols

Discipline Roadmap for: WAN/LAN Protocols



Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

WAN Protocols

- Frame Relay → (to 2 Years)
- ATM → (to 2 Years)
- SNA → Containment Targets
- Ethernet → (to 2 Years)

MPLS (2 Years) → (to 5 Years)

LAN Protocols

- Ethernet
- Gigabit Ethernet
- TCP/IP
- IPX/SPX
- LAT-DEC
- SNA
- AppleTalk

Ethernet, Gigabit Ethernet → Ethernet (Switched) → (to 5 Years)

TCP/IP → TCP/IP → (to 5 Years)

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

WAN:
ATM, Frame Relay, Ethernet, MPLS

LAN:
Ethernet (switched), TCP/IP

Containment Targets

SNA (WAN), SNA (LAN), IPX/SPX, AppleTalk, LAT-DEC

Emerging Platforms

MPLS

Implications and Dependencies

Individual agencies should conduct an evaluation for moving applications from SNA to current technologies.

Roadmap Notes

A business case analysis will be conducted to determine the timing of scheduling SNA for retirement. SNA investments should be curtailed pending completion of this business case analysis.

DISCIPLINE: WAN/LAN Protocols (Cont'd)

Discipline Roadmap for: WAN/LAN Protocols

- **Discipline Boundaries:**
  - WAN/LAN
- **Discipline Standards:**
  - None.
- **Migration Considerations:**
  - Those agencies with SNA networks should consider converting to IP Network when feasible.
- **Exception Considerations:**
  - None.
- **Miscellaneous Notes:**
  - May want to establish another Discipline for WAN Transport in the future.
- **Established Date:**
  - April 28, 2004
- **Date Last Reviewed:**
  - July 26, 2006
- **Next Review Date:**
  - July 2007

DISCIPLINE: Hardware— Switches & Routers

Discipline Roadmap for: Switches & Routers

DOMAIN: COMMUNICATION SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Switches 3COM switches 6506 Switch Cisco Switches catalyst (2916, 2924, 4003, 4006, 6513, 3550) DMV Core Switches Nortel Accelar 1150R-B Nortel Switches (350,450) Enterasys Avaya HP	Cisco Nortel Enterasys HP	Market Watch
Routers 6506 Switch/Router Cisco 4000 Routers Cisco Routers (1650,2500, 2600, 2620, 3660, 3600, 1750, DSL Cisco 840) Nortel ARNs	Cisco Nortel Enterasys HP	

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

Cisco, Nortel, Enterasys, HP

Containment Targets

3COM, Avaya

Emerging Platforms

Implications and Dependencies

Only select from products that support industry standards.

Roadmap Notes

Identify industry standards

DISCIPLINE: Hardware— Switches & Routers (Cont'd)

Discipline Roadmap for: Switches & Routers

- **Discipline Boundaries:**
  - Equipment room, MDF-IDF equipment. Only wiring closets.
- **Discipline Standards:**
  - IETF routing standards.
- **Migration Considerations:**
  - TBD
- **Exception Considerations:**
  - TBD
- **Miscellaneous Notes:**
  - None.
- **Established Date**
  - October 16, 2003
- **Date Last Updated:**
  - July 26, 2006
- **Next Review Date:**
  - July 2007

DISCIPLINE: Remote Access Methods & Clients

Discipline Roadmap for: Remote Access Methods & Clients

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Remote Access Methods VPN Remote Access Server (dial up)	IPSec VPN → SSL →	
Clients SSL Client Citrix Metaframe XPA Cisco VPN Client Nortell VPN Client	Client is dependent upon remote access method.	

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

IPSec VPN, and SSL

Containment Targets

Direct Dial (Back-up or maintenance Access)

Emerging Platforms

Implications and Dependencies

Discipline is dependent upon the results of the Security Subcommittee disciplines. Managed services for access to agency networks should adhere to the IPSec VPN & SSL industry standards.

Roadmap Notes

We will review this discipline when the Security Subcommittee has published its disciplines.

DISCIPLINE: Remote Access Methods & Clients (Cont'd)

Discipline Roadmap for: Remote Access Methods & Clients

- **Discipline Boundaries:**
  - ❑ Remote Access to individual agency's networks.
- **Discipline Standards:**
  - ❑ Restricted to approved industry standards.
- **Migration Considerations:**
  - ❑ Agency dependent.
- **Exception Considerations:**
  - ❑ Secured direct dial access may be acceptable when no other network access is available.
- **Miscellaneous Notes:**
  - ❑ None
- **Established Date:**
  - ❑ December 15, 2004
- **Date Last Updated:**
  - ❑ July 26, 2006
- **Next Review Date:**
  - ❑ July 2007

DISCIPLINE: LAN Topologies

Discipline Roadmap for: LAN Topologies

DOMAIN: COMMUNICATION SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
100 Mb HD Shared Ethernet 100Mb FD Switched Ethernet Collapsed Backbone Ethernet-100 Ethernet 10/100 Gigabit Switched Ethernet IBM Token Ring	Ethernet (Switched)	

Shared	Agency
✓	✓

Retirement Targets

Token Ring

Mainstream Platforms (must be supported)

Ethernet

Containment Targets

Emerging Platforms

Implications and Dependencies

Minimum 100 Mb

Roadmap Notes

DISCIPLINE: LAN Topologies (Cont'd)

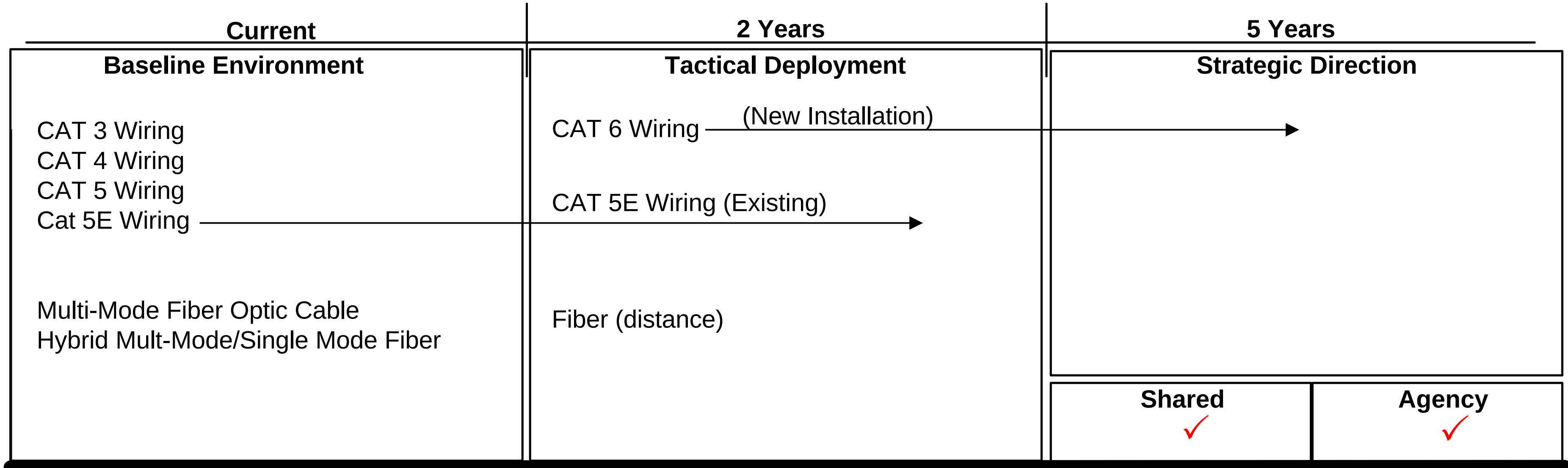
Discipline Roadmap for: LAN Topologies

- **Discipline Boundaries:**
  - TBD
- **Discipline Standards:**
  - TBD
- **Migration Considerations:**
  - TBD
- **Exception Considerations:**
  - TBD
- **Miscellaneous Notes:**
  - None.
- **Next Review Date**
  - July 2007
- **Established Date**
  - October 8, 2003
- **Date Last Updated:**
  - July 26, 2006

DISCIPLINE: LAN Wiring

Discipline Roadmap for: LAN Wiring

DOMAIN: COMMUNICATION SERVICES



Current

Baseline Environment

CAT 3 Wiring
CAT 4 Wiring
CAT 5 Wiring
Cat 5E Wiring

Multi-Mode Fiber Optic Cable
Hybrid Mult-Mode/Single Mode Fiber

2 Years

Tactical Deployment

CAT 6 Wiring (New Installation)

CAT 5E Wiring (Existing)

Fiber (distance)

5 Years

Strategic Direction

Shared	**Agency**
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

CAT 5E, CAT 6

Containment Targets

CAT 3, CAT 4, CAT 5

Emerging Platforms

Wireless LANs

Implications and Dependencies

Roadmap Notes

Need LAN Wiring specification template

DISCIPLINE: LAN Wiring (Cont'd)

Discipline Roadmap for: LAN Wiring

- **Discipline Boundaries:**
  - ❑ Building wiring horizontals and verticals.
- **Discipline Standards:**
  - ❑ National Electric Code, BICSI method, TIA. See proposed SC LAN wiring standards.
- **Migration Considerations:**
  - ❑ Replace as required.
- **Exception Considerations:**
  - ❑ TBD
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ October 8, 2003
- **Date Last Reviewed:**
  - ❑ July 26, 2006
- **Next Review Date:**
  - ❑ July 2007

DISCIPLINE: Wireless LAN Protocols

Discipline Roadmap for: Wireless LAN Protocols

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Protocol 802.11a → 802.11b → 802.11g →	→	Market Watch
		Shared
		Agency ✓

Retirement Targets

Mainstream Platforms (must be supported)

802.11a/b/g

Containment Targets

Emerging Platforms

802.11n

Implications and Dependencies

Roadmap Notes

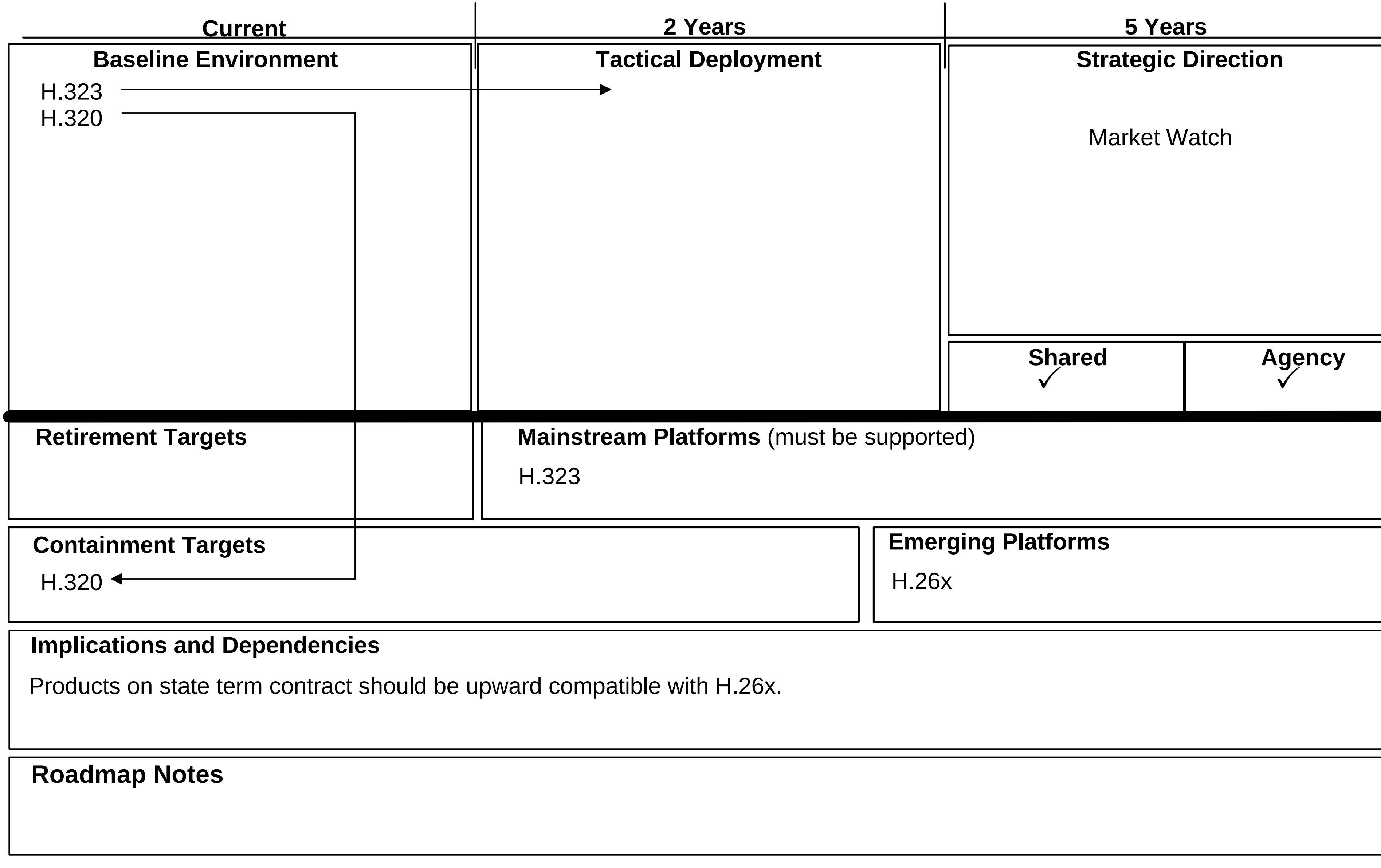
DISCIPLINE: Wireless LAN Protocols (Cont’d)

Discipline Roadmap for: Wireless LAN Protocols

- **Discipline Boundaries:**
  - This standard is for agency LAN access.
- **Discipline Standards:**
  - Restricted to approved ITE industry standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - Agencies should be aware of security risks involved with using wireless communications.
- **Established Date:**
  - December 15, 2004
- **Date Last Updated:**
  - July 26, 2006
- **Next Review Date:**
  - July 2007

DISCIPLINE: Enterprise Telecommunications Video

Discipline Roadmap for: Video



Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
H.323 →	→	
H.320		Market Watch
		Shared ✓
		Agency ✓

Retirement Targets

Mainstream Platforms (must be supported)

H.323

Containment Targets

H.320

Emerging Platforms

H.26x

Implications and Dependencies

Products on state term contract should be upward compatible with H.26x.

Roadmap Notes

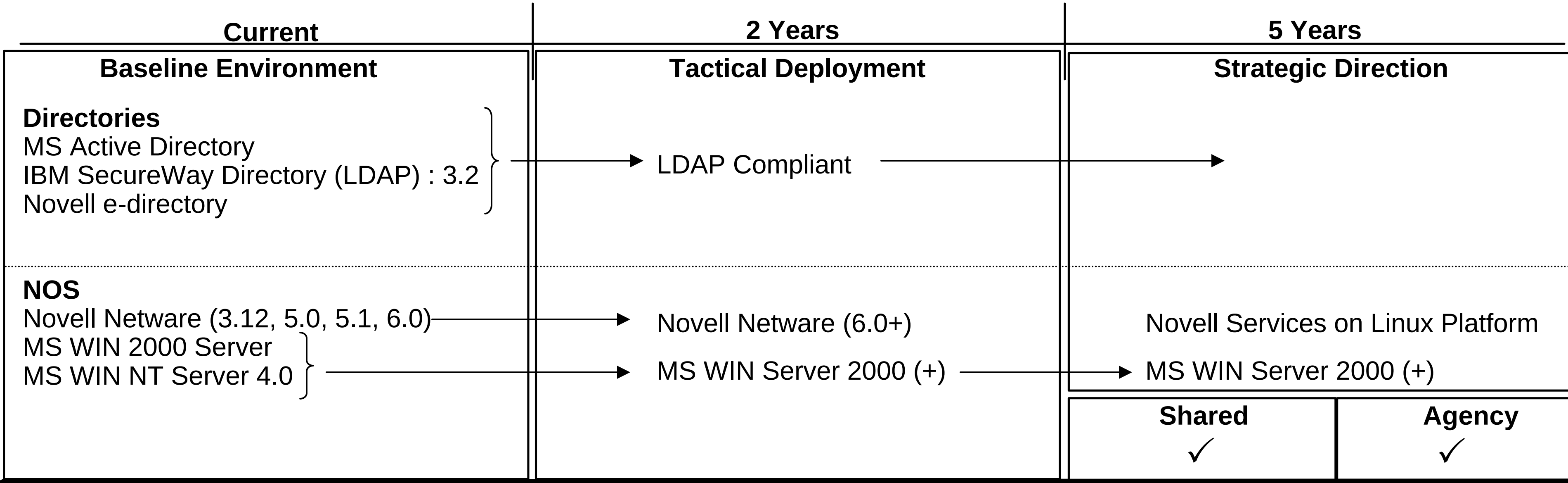
DISCIPLINE: Enterprise Telecommunications (Cont’d)

Discipline Roadmap for: Video

- **Discipline Boundaries:**
  - ❑ Protocol for inter-agency video communications.
- **Discipline Standards:**
  - ❑ H.323
- **Migration Considerations:**
  - ❑ There is a large installed base of H.320 that exists in South Carolina State Government. As this base becomes obsolete, it should be replaced with H.323.
- **Exception Considerations:**
  - ❑ H.320 is acceptable when needed for compatibility with other systems or IP is not availability.
- **Miscellaneous Notes:**
  - ❑ Gateways between H.320 and H.323 are available.
- **Established Date**
  - ❑ August 25, 2004
- **Date Last Updated:**
  - ❑ July 26, 2006
- **Next Review Date:**
  - ❑ July 2007

DISCIPLINE: Directory, Network OS

Discipline Roadmap for: Directory, Network OS



Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Directories MS Active Directory IBM SecureWay Directory (LDAP) : 3.2 Novell e-directory	LDAP Compliant	
NOS Novell Netware (3.12, 5.0, 5.1, 6.0) MS WIN 2000 Server MS WIN NT Server 4.0	Novell Netware (6.0+) MS WIN Server 2000 (+)	Novell Services on Linux Platform MS WIN Server 2000 (+)
		Shared ✓ **Agency** ✓

Retirement Targets

Mainstream Platforms (must be supported)

Novell Netware (6.0+), MS WIN Server 2000(+)

Containment Targets

Novell Netware (pre 6.0), MS WIN NT Server

Emerging Platforms

Implications and Dependencies

Novell is moving from Netware platform to SUSE Linux platform.

Roadmap Notes

.

DISCIPLINE: Directory, Network OS (Cont'd)

Discipline Roadmap for: Directory, Network OS

- **Discipline Boundaries:**
  - ❑ Network OS limited to agency networks. Directory services limited to shared directories.
- **Discipline Standards:**
  - ❑ Directories must be LDAP compliant.
- **Migration Considerations:**
  - ❑ Agencies should research and plan for migration path in regards to Novell strategy.
- **Exception Considerations:**
  - ❑ None
- **Miscellaneous Notes:**
  - ❑ None
- **Date Last Updated:**
  - ❑ January 26, 2005
- **Date Last Updated:**
  - ❑ July 26, 2006
- **Next Review Date:**
  - ❑ July 2007

DISCIPLINE: e-Mail Services

Discipline Roadmap for: e-Mail Services

Current	2 Years	5 Years

Baseline Environment

MS Exchange
MS Exchange 2000
MS Exchange 5.5
Novell Groupwise
Novell GroupWise 5.5
Novell GroupWise 6
Novell GroupWise (5, 6) Internet Agent
Novell GroupWise (5, 6) Webaccess Agent
Lotus Domino
Sendmail

Tactical Deployment

(Based on business needs)

Strategic Direction

Market watch

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms

MS Exchange, GroupWise

Containment Targets

Lotus Domino, SendMail

Emerging Platforms

Implications and Dependencies

Roadmap Notes

Need web access to check email remotely

DISCIPLINE: e-Mail Services (Cont'd)

Discipline Roadmap for: e-Mail Services

- **Discipline Boundaries:**
  - N/A
- **Discipline Standards:**
  - As stated under tactical deployment
- **Migration Considerations:**
  - Recommendations for migration to the recommended standards will be made upon completion of the business case analysis on an agency by agency basis.
- **Exception Considerations:**
  - N/A
- **Miscellaneous Notes:**
  - Need continuous input from the Security Domain Subcommittee.
- **Established Date**
  - April 28, 2004
- **Date Last Updated:**
  - July 26, 2006
- **Next Review Date:**
  - July 2007

E-MAIL BASELINE

In May of this year, the Division of the State CIO conducted a survey of the various e-mail systems currently in use in South Carolina state government. The survey, which was done at the request of the State Architecture Oversight Committee (AOC), was completed on June 15, 2004. The findings are presented below.

GroupWise

Agency	# of Users
Attorney General	250
Consumer Affairs	47
DHEC	5000
Dept. Mental Health	3704
Dept. Health & Human Serv.	2000
Dept. of Education	795
Dept. of Revenue	750
Div. of State CIO	371
Election Commission	20
Ethics Commission	9
General Services	300
Governor's Office OEPP	250
Human Affairs	46
Human Resources	45
Insurance Department	100
John de la Howe	65
Research & Statistical Serv.	80
Second Injury Fund	23
(18 agencies)	13,855

Other Systems

Agency	# of Licenses
Appellate Defense (*InfoAve.com*)	14
Comm. on Prosecution	10
DSS (*Lotus Notes*)	3500
Minority Affairs Commission	7
Procurement Review Panel (*Earthlink*)	2
Sea Grants Consortium (*MS Outlook*)	15
Sec. of State (*MS Outlook Express*)	15
State Library (*SMTP/Multinet*)	48
Tech & Comp Educ Bd (*MS Outlook*)	100
Tuition Grants (*MS Outlook*)	4
(10 agencies)	3,715

MS Exchange

Agency	# of Users
Admin. Law Judge Div.	20
Archives & History	100
Dept. of Commerce	150
Commission for the Blind	150
Comptroller General	73
Dept. Alcohol & Drug Abuse	80
Dept. Disabilities & Sp. Needs	750
Dept. Motor Vehicles	1500
Dept. Natural Resources	715
Dept. of Corrections	750
Dept. of Transportation	2600
Forestry Commission	120
Higher Education Comm.	60
Housing Dev't. Auth.	125
Insurance Department	100
Judicial Department	650
Legislative Audit Council	15
Labor, Licensing & Regulation	400
Lottery Commission	150
Patriot's Point	140
Parks, Recreation and Tourism	330
Public Service Comm.	82
Retirement Systems	300
SLED	510
State Accident Fund	100
State Auditor	56
State Museum	150
Vocational Rehabilitation	1000
Wil Lou Gray Opp. School	68
Worker's Compensation	58
(30 agencies)	11,302

GroupWise

Schools	# of Users
MUSC	6000
USC	6300
(2 schools)	12,300

Other Systems

Schools	# of Licenses
Cent. Car. Tech (*Campus Pipeline*)	4000
Citadel (*Stalker's Communigate*)	3000
Clemson (*Eudora, MS Outlook, Pegasus, Netscape Mail, SquirrelMail, MacOS X, Unix/Linux system*)	57,500
Coastal Carolina (*Sendmail*)	13,485
College of Charleston (*Sendmail*)	12,000
Francis Marion Univ (*TMDF/DEC*)	600
Horry-Georgetown Tech (*iPlanet*)	12,713
MUSC (*IMAP/Esys*)	2500
Tri-County Tech (*Netscape*)	11,000
Winthrop University (*IPSwitch*)	6000
(10 schools)	122,798

MS Exchange

Schools	# of Users
Aiken Tech	200
Central Carolina Tech	350
College of Charleston	1500
Denmark Tech	70
Horry-Georgetown Tech	421
Midlands Tech	1550
Northeast Tech	130
Orangeburg-Calhoun Tech	250
Spartanburg Tech	500
SC State University	5000
Tech. Col. of the Low Cntry.	200
Trident Tech	1465
Williamsburg Tech	60
Winthrop Univ.	1000
York Tech	300
(15 schools)	12,996

July 8, 2004

DOMAIN: SECURITY

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection – Desktop/Server

Current

Baseline Environment

Desktop/Workstation

McAfee Anti Virus
Trend Micro (Anti-virus)
Norton Antivirus
CA eTrust
F-Prot
Sophos

2 Years

Tactical Deployment

McAfee
Trend Micro
Symantec (Norton)
CA eTrust (inoculator)

5 Years

Strategic Direction

Those products that contain integrated anti-virus with centralized management.

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

McAfee, Trend Micro, Symantec (Norton), CA eTrust

Containment Targets

F-Prot, Sophos

Emerging Platforms

MS Windows Live OneCare

Implications and Dependencies

Independent of the perimeter virus protection. New signature files and signature updates must be kept current. Vendor must deliver consolidated management console.

Roadmap Notes

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection – Desktop/Server

- **Discipline Boundaries:**
  - ❑ To be used at the Desktop or on a Server. For, example virus protection running on the employee’s desktop that scans the email prior to the email software opening the attached file.

- **Discipline Standards:**

- **Migration Considerations:**

- **Exception Considerations:**

- **Miscellaneous Notes:**
  - ❑ There are no virus protection protocols.

- **Established**
  - ❑ August 25, 2004

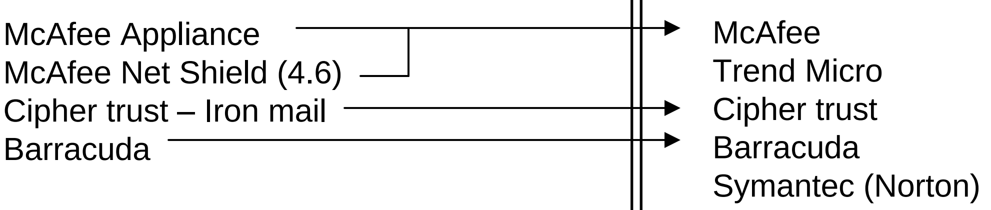
- **Date Last Updated:**
  - ❑ August 23, 2006

- **Next Review Date:**
  - ❑ August 2007

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection - Perimeter

DOMAIN: SECURITY



Current

Baseline Environment

McAfee Appliance
McAfee Net Shield (4.6)
Cipher trust – Iron mail
Barracuda

2 Years

Tactical Deployment

McAfee
Trend Micro
Cipher trust
Barracuda
Symantec (Norton)

5 Years

Strategic Direction

Market Watch

Additional functionality (e.g., spyware, antispam) included into perimeter packages

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

McAfee, Trend Micro, Symantec, Cipher Trust, Barracuda

Containment Targets

Emerging Platforms

Implications and Dependencies

Independent of the desktop/server virus protection. New signature files and signature updates must be kept current. Vendor must deliver consolidated management console.

Roadmap Notes

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection - Perimeter

- **Discipline Boundaries:**
  - To be used as a perimeter device which refers to the logic position within the agencies network. For example, an email virus protection appliance where all email is scanned prior to being accessed by the employee's at their desktops.
- **Discipline Standards:**
- **Migration Considerations:**
- **Exception Considerations:**
- **Miscellaneous Notes:**
  - There are no virus protection industry protocols.
- **Established**
  - August 25, 2004
- **Date Last Updated:**
  - August 23, 2006
- **Next Review Date:**
  - August 2007

DOMAIN: SECURITY

DISCIPLINE: Host Protection

Discipline Roadmap for: Anti-Spyware

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

Baseline Environment

Host-based

- Websense
- McAfee
- LavaSoft
- Microsoft
- Sunbelt
- Symantec
- PC Tools (unmanaged)
- Spybot Search and Destroy

Network-based

- LavaSoft
- Barracuda
- Intrusion Inc. (SpySnare)
- SonicWALL

Root Kit Defense

- Microsoft
- Backlight Defender

Tactical Deployment

Strategic Direction

Market watch for consolidated products.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

This market is poised for significant consolidation.

Implications and Dependencies

- Centralized management and administration of host-based clients.
- It is highly recommended that multiple products be used in concert in order to create an in-depth defense since not all products defend equally.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Host Protection

Discipline Roadmap for: Anti-Spyware

- **Discipline Boundaries:**
  - Spyware is a broad category of software designed to subvert a computer's operation for the benefit of a third party, without the informed consent of the owner. Spyware may be malicious in nature, intending to collect financial information for identify-theft or it can be relatively benign, originating form legitimate companies for the intended purpose of advertising. Anti-spyware is software that is designed to remove or block spyware.
- **Discipline Standards:**
  - Currently, there are no anti-spyware specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - Entities should consider restricting intentional downloading and installation of programs.
  - Entities should consider providing training to educate users in areas, such as:
    - Understanding of End User License Agreement (EULA), since often times agreements to install spyware are included in the fine print.
    - Proper response to pop-up windows.
    - Recognition of spyware symptoms.
    - Awareness of suspicious emails and "free" software.
  - Entities should consider tightening browser security, e.g. disabling Active X.
  - Entities should consider installing pop-up blockers.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DOMAIN: SECURITY

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: Email Protection (SPAM)

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
IronPort Systems Symantec McAfee Trend Micro Secure Computing (Cipher Trust) MicroSoft SonicWall Barracuda		Market Watch – Consolidation into a unified threat management device.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

This market is poised for significant consolidation.

Implications and Dependencies

- SonicWall and Barracuda are recommended for mid-size (1,000 units) and small enterprises.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: Email Protection (SPAM)

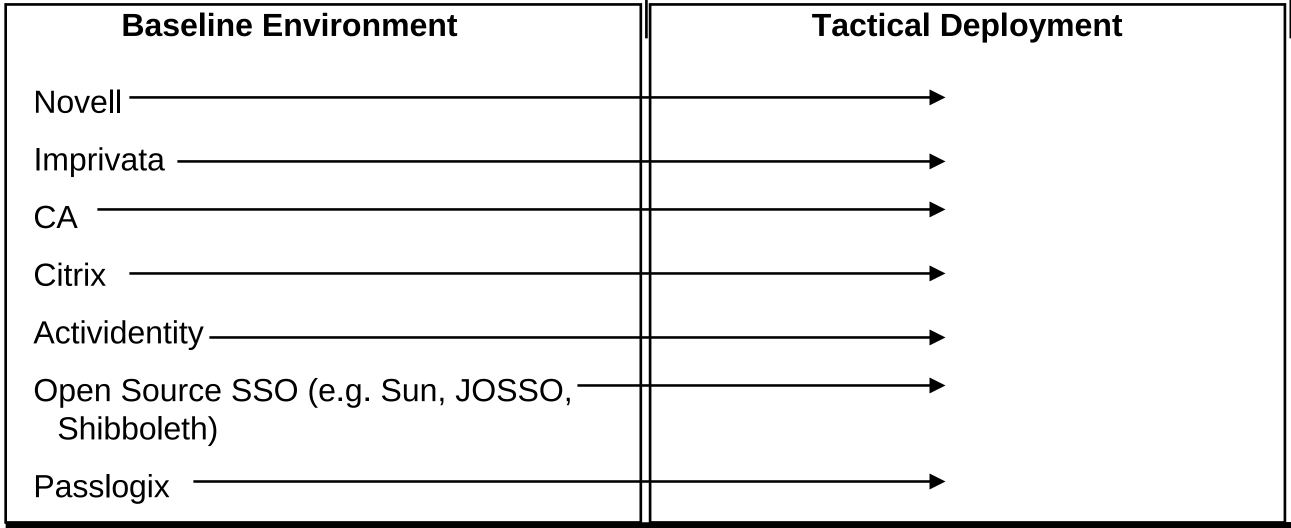
- **Discipline Boundaries:**
  - Spamming is the abuse of electronic messaging systems to send unsolicited, undesired, bulk messages. Email spam involves sending nearly identical messages to a few or millions of email recipients without permission. Spammers often harvest addresses from web pages, databases or by employing educated guessing.
- **Discipline Standards:**
  - Currently, there are no SPAM specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Identification and Authentication

Discipline Roadmap for: Enterprise Single Sign-On (ESSO)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**



Novell

Imprivata

CA

Citrix

Actividentity

Open Source SSO (e.g. Sun, JOSSO, Shibboleth)

Passlogix

Strategic Direction

Market watch of ESSO and IAM (identity and access management) best practices and solutions.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Novell, Imprivata, CA, Citrix, Actividentity, Open Source SSO, Passlogix

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- User access and authorization through RDMS or LDAP based systems.
- Management through SNMPv3 or IP.

Roadmap Notes

- Standard to reviewed annually after adoption by the AOC.

DISCIPLINE: Identification and Authentication

Discipline Roadmap for: Enterprise Single Sign-On (ESSO)

- **Discipline Boundaries:**
  - ❑ Enterprise Single Sign-On refers to specialized software that enables a user to authenticate once and gain access to multiple, often disparate, technology targets (e.g. network, web, and windows interfaces). ESSO is part of a larger segment of tools known as identity and access management (IAM), but it is differentiated from similar technologies (such as password wallets, password synchronization, and directory sign-on) because it is centrally administered on an enterprise level, provides automatic log on, and allows for legacy applications that are not directory-enabled.
- **Discipline Standards:**
  - ❑ Currently, there are no generally accepted independent standards. Instead, ESSO tools are proprietary, although some use XML as an integral part of their system. However, the Federal Government has adopted the Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) as its base standard.
- **Migration Considerations:**
  - ❑ Migration can be expensive and time consuming.
  - ❑ Positive ROI, through user and helpdesk time savings, is generally not realized unless an entity has several heterogeneous applications requiring daily sign-on with individualized credentials.
  - ❑ Can be coupled with other authentication methods, such as biometrics or smart cards, to provide stronger authentication in order to address concerns that a compromise of the master password likewise compromises all target systems.
  - ❑ Consider “webifying” legacy applications in order to exploit WAM (web access management) products as newer applications are usually natively web-enabled.
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should to be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ None
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DOMAIN: SECURITY

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Facility Access and Monitoring Systems

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

Baseline Environment

Access Systems

- Biometric
- Proximity
- Code-based

Surveillance

- Closed-Circuit
- IP-based

Tactical Deployment

Strategic Direction

Market Watch

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- User access and authorization through database or LDAP based systems. Management through SNMPv3 or IP.
- Should be incorporated into the entity’s power redundancy strategy.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Facility Access and Monitoring Systems

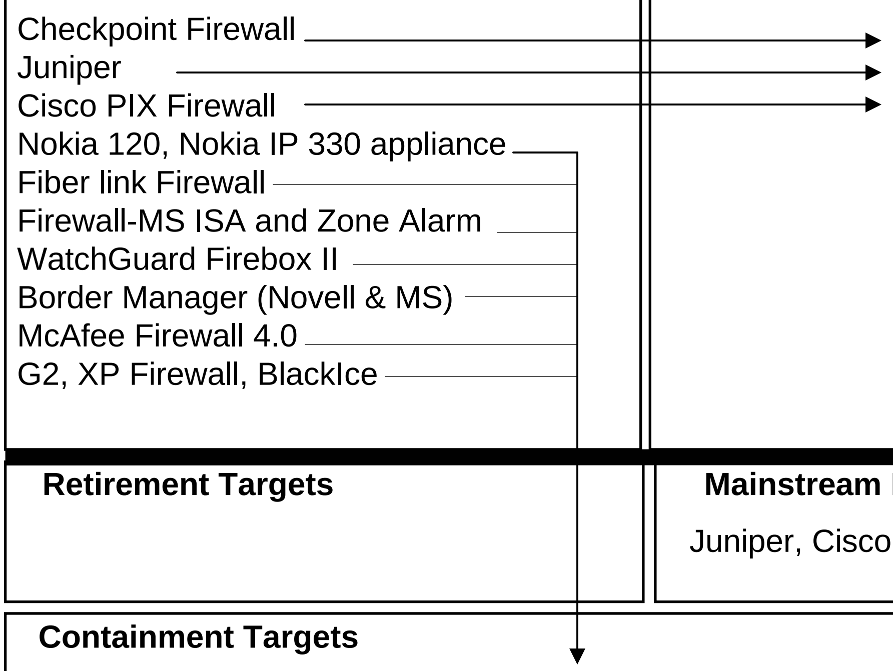
- **Discipline Boundaries:**
  - ❑ Barrier defense systems (e.g. key card, PIN entry, finger print biometrics, retinal scans, facial recognition, etc.) used to secure restricted access areas (e.g. server room, entity campus), as well as monitoring systems for surveillance (e.g. Closed Circuit TV). Does not address “boots on the ground” security personnel.
- **Discipline Standards:**
  - ❑ Must support the SC Enterprise Architecture standards for networking (e.g. LAN, WAN, cabling, etc.).
- **Migration Considerations:**
  - ❑ None
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ Should be implemented in a layered approach to provide failsafes:
    - Surveillance layer - e.g. cameras, motion detectors, and microphones
    - Access Control layer – e.g. key and keyless locks, biometrics, etc.
    - Infrastructure layer – e.g., windows, doors, locks, etc.
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DOMAIN: SECURITY

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Firewalls

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**



Checkpoint Firewall
Juniper
Cisco PIX Firewall
Nokia 120, Nokia IP 330 appliance
Fiber link Firewall
Firewall-MS ISA and Zone Alarm
WatchGuard Firebox II
Border Manager (Novell & MS)
McAfee Firewall 4.0
G2, XP Firewall, BlackIce

Strategic Direction

Firewall with enhanced deep packet inspection.

Deperimeterization requires defense in layers strategy.

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms

Juniper, Cisco PIX, Checkpoint

Containment Targets

Contain everything else with one footnote (see below)

Emerging Platforms

Enhanced deep packet inspection & evolving multipurpose security w/ increased functionality.

Implications and Dependencies

Deep packet inspection (DPI) is viewed as a must have feature because of the increasing blended attacks even in the tactical deployment. Perimeter firewalls that do not have DPI or limited DPI should be augmented with an intrusion prevention device.

Roadmap Notes

- Nokia H/W appliance running Checkpoint is valid for implementation.
- The committee plans to review this discipline yearly during August.

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Firewalls

- **Discipline Boundaries:**
  - While separate disciplines, desktop firewalls and perimeter firewalls are not mutually exclusive of one another. The best implementation strategy would be a layered approach with a strong perimeter defense supplemented by a strong desktop defense. In many instances, you would model the firewall strategy after the evolution of the anti-virus strategy with at least a clear two tier approach. In some cases, additional firewalls or IPS implementations would be necessary to protect extremely sensitive data from both internal and external threats and to provide a third tier. Each implementation is situational with at least a deep packet inspection (DPI) perimeter solution.

- **Discipline Standards:**

- **Migration Considerations:**
  - Should an agency convert to a recommended firewall products, expect a price of $5K to $15K. This is the current price with deep packet inspection and VPN capabilities with four 10/100 network connections.

- **Exception Considerations:**

- **Miscellaneous Notes:**

- **Established Date**
  - April 28, 2004

- **Date Last Updated:**
  - August 23, 2006

- **Next Review Date:**
  - August 2007

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Desktop Firewalls

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Zone Alarm (Checkpoint) → McAfee → Symantec → MS Firewall → BlackIce		Those that contain integrated anti-virus with centralized management. Enhanced centralized management continuingly evolving.

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms

Zone Alarm, McAfee, Symantec

Containment Targets

BlackIce

Emerging Platforms

– Desktop IPS in tandem w/Desktop Firewalls or as an IDS replacement or supplement.
– MS Firewall

Implications and Dependencies

Roadmap Notes

– The committee plans to review this discipline yearly during August.

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Desktop Firewalls

- **Discipline Boundaries:**
  - ❑ While separate disciplines, desktop firewalls and perimeter firewalls are not mutually exclusive of one another. The best implementation strategy would be a layered approach with a strong perimeter defense supplemented by a strong desktop defense. In many instances, you would model the firewall strategy after the evolution of the anti-virus strategy with at least a clear two tier approach. In some cases, additional firewalls or IPS implementations would be necessary to protect extremely sensitive data from both internal and external threats and to provide a third tier. Each implementation is situational with at least a deep packet inspection (DPI) perimeter solution.
- **Discipline Standards:**
- **Migration Considerations:**
- **Exception Considerations:**
- **Miscellaneous Notes:**
- **Established Date**
  - ❑ April 28, 2004
- **Date Last Updated:**
  - ❑ August 23, 2006
- **Next Review Date:**
  - ❑ August 2007

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: HVAC (Heating, Ventilating, and Air Conditioning)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Liebert →		Market Watch (green refrigerants and waterless refrigerants)
Most data center purposed equipment for room, zone and rack level systems, supported by 24x7x365 support, are acceptable.		

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Liebert

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- Acquisition costs can be significant.
- External assessment recommended to determine capacity requirements. (Reference State Engineer's Office existing contract)

Roadmap Notes

- Network-based power management systems must be secured with at least SNMPv3.

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: HVAC (Heating, Ventilating, and Air Conditioning)

- **Discipline Boundaries:**
  - ❑ HVAC specific to data center applications, may include rooftop units and distributed units that provide localized air cooling, or under-floor systems used in conjunction with raised floor areas.
- **Discipline Standards:**
  - ❑ ANSI 135 - BACnet Data Communication for Building Automation and Control Networks.
  - ❑ "Telecommunications Infrastructure Standard for Data Centers," TIA-942
- **Migration Considerations:**
  - ❑ Should be an integrated system that optimizes electrical power, space allocation and mechanical systems.
  - ❑ Strive for redundancy in the HVAC system by installing multiple units; focus on rack and tile placement to maximize the efficient flow of chilled air; use spot cooling as needed.
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ HVAC should be integrated with a humidity control system.
  - ❑ Design guidelines:
    - – Ambient temperature should be between 70° and 72° F, with a relative humidity of 45% to 50%.
    - – Redundant (distributed units) systems are better than centralized systems.
    - – Design airflow to move from bottom to top and from front to back through racks to avoid consumption of used air.
    - – Alternate cold-aisle and hot-aisle (intakes facing each other, exhaust facing each other) for temperature control efficiencies.
    - – Establish a vapor barrier throughout the perimeter of the data center to minimize condensation.
    - – Use spot cooling or special rack enclosures for hot spots in the data center layout.
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DOMAIN: SECURITY

DISCIPLINE: Host Protection

Discipline Roadmap for: Host-based Intrusion Prevention System (HIPS)

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

McAfee Entercept

Symantec

Cisco

ISS

Sana

AppArmor (Linux)

Market Watch of a single multi-function threat management client.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

McAfee Entercept, Symantec, Cisco, ISS, Sana, AppArmor

Containment Targets

N/A

Emerging Platforms

Consolidation into a single multi-function threat management client.

Implications and Dependencies

- Centralized management and administration of host-based clients.
- It is highly recommended that multiple products be used in concert in order to create an in-depth defense since not all products defend equally.

Roadmap Notes

- Certain products listed may be better suited for server or desktop dependent on use-case.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Host Protection

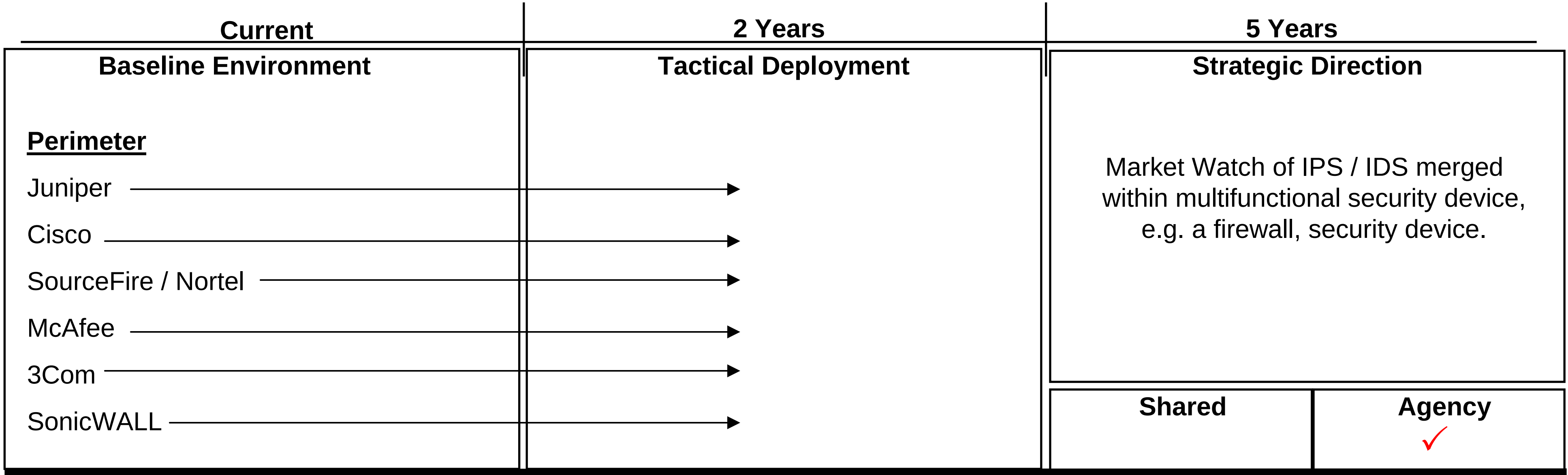
Discipline Roadmap for: Host-based Intrusion Prevention System (HIPS)

- **Discipline Boundaries:**
  - An IPS is any device which exercises control to protect networks, applications and computers from exploitation. IPS are intended to resolve ambiguities in passive network monitoring by placing detection in-line. There are 4 basic types of IPS: host-based network, content-based, and rate-based (the last 3 are addressed in a separate roadmap). Host-based IPS (HIPS) systems reside on a specific IP address, such as a PC system.
- **Discipline Standards:**
  - Currently, there are no HIPS specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: IPS (Intrusion Prevention System) / IDS (Intrusion Detection System)

DOMAIN: SECURITY



Current | **2 Years** | **5 Years**

Baseline Environment

Perimeter

Juniper →

Cisco →

SourceFire / Nortel →

McAfee →

3Com →

SonicWALL →

Tactical Deployment

Strategic Direction

Market Watch of IPS / IDS merged within multifunctional security device, e.g. a firewall, security device.

Shared	**Agency**
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Juniper, Cisco, SourceFire / Nortel, McAfee, 3Com, SonicWall

Containment Targets

N/A

Emerging Platforms

IPS / IDS merged w/in multifunctional security device, e.g. a firewall, security device.

Implications and Dependencies

- Costs and implementation considerations can be substantial (~$30-$150k).
- SNMP v3

Roadmap Notes

- IDS still valid for asynchronous forensics.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: IPS (Intrusion Prevention System) / IDS (Intrusion Detection System)

- **Discipline Boundaries:**
  - ❑ An IPS is any device which exercises control to protect networks, applications and computers from exploitation. IPS are intended to resolve ambiguities in passive network monitoring by placing detection in-line. There are 4 basic types of IPS: host-based (addressed in its own roadmap), network, content-based, and rate-based. Network IPS (NIPS) are designed to inspect traffic and can drop malicious traffic. Content-based IPS are designed to inspect network packets and can avoid infections and hacks. Rate-based IPS are designed to prevent denial of services attacks.
  - ❑ An IDS is a device which is used to detect all types of malicious network traffic and computer usage that can’t be detected by conventional firewalls. An IDS differs from an IPS mainly in that it requires much more human involvement and is implemented near-line instead of in-line.
- **Discipline Standards:**
  - ❑ Currently, there are no IPS or IDS specific standards.
- **Migration Considerations:**
  - ❑ The biggest problem with IPS/IDS is false reports, either false positives (alerts w/o validity) or false negatives (no alerts when actual threats exist). Both problems are typically due to tuning issues, under or over tuning respectively. Because neither system can completely avoid false reports, it is recommended that tuning err towards false negatives, given the inherently greater consequences.
  - ❑ IDS tends to have higher manpower costs, while IPS tends to have functionality risks.
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ None
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Network Access Control (NAC)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
MS Cisco Juniper TCG ConSentry		Market Watch

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- None

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Network Access Control (NAC)

- **Discipline Boundaries:**
  - None
- **Discipline Standards:**
  - None
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Power Management

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

Baseline Environment

Desktop

- APC (Schneider Electric, SA)
- Tripp Lite

Data Center

- Battery-based
  - APC (Schneider Electric, SA)
  - Liebert
- Fly-wheel
  - Caterpillar
  - Pentadyne

Tactical Deployment

Strategic Direction

Market Watch

(DC Power Systems and "Green" Systems)

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Desktop: APC. Tripp Lite, Data Center: APC, Liebert, Caterpillar, Pentadyne

Containment Targets

N/A

Emerging Platforms

DC Power Systems, "Green" Systems

Implications and Dependencies

- Use backup generators for anticipated outages in excess of 20 minutes, UPS (uninterruptible power supply) for outage up to 20 minutes, and surge protection for unprotected systems.

Roadmap Notes

- Network-based power management systems must be secured with at least SNMPv3.

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Power Management

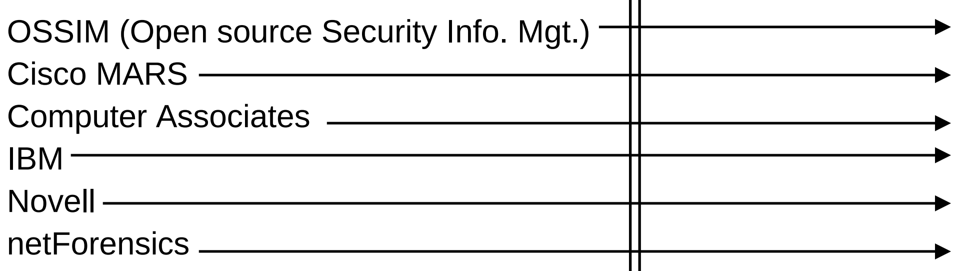
- **Discipline Boundaries:**
  - ❑ Redundant power sources specific to data center and desktop applications, including: uninterruptible power supply (UPS) and backup generators.
- **Discipline Standards:**
  - ❑ IEEE Emerald Book (data and electrical grounding)
  - ❑ IEEE Green Book (commercial grounding)
  - ❑ NEBS (Network Equipment Building Standards)
- **Migration Considerations:**
  - ❑ New data center designs should balance environmental efficiency with computing needs.
  - ❑ UPS should be sized to power 100% of "peak" load (or fault overload) of equipment until backup power kicks in.
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should to be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ Typical needs range from 30 to 70 watts/ft.^{2} for computing equipment, plus additional power for HVAC, humidification, lighting and transformer losses.
  - ❑ Use the Uptime Institute's fault tolerance levels for data centers to balance capital costs and service requirements:
    - Tier 1: Single path for power and cooling distribution; no redundant components - < 28.8 hours of downtime/year
    - Tier 2: Single path for power and cooling distribution; redundant components - < 22.0 hours of downtime/year
    - Tier 3: Multiple paths for power and cooling distribution; concurrently maintainable redundant components - < 1.6 hours of downtime/year
    - Tier 4: Multiple paths for power and cooling distribution; fault tolerant redundant components - < 0.4 hours of downtime/year
    - Tiers 3 & 4 (fault tolerant) will require backup generators.
  - ❑ Backup Generator considerations include:
    - Compliance with local fuel storage and noise abatement code.
    - Exhaust and vibration effects.
    - Maintenance and fuel contracts.
    - Plans for periodic testing.
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DOMAIN: SECURITY

DISCIPLINE: Confidentiality and Integrity

Discipline Roadmap for: SIEM (Security Information & Event Management)

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**



OSSIM (Open source Security Info. Mgt.)

Cisco MARS

Computer Associates

IBM

Novell

netForensics

Strategic Direction

Market Watch

Shared	**Agency**
✓	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

OSSIM, Cisco MARS, Computer Associates, IBM, Novell, netForensics

Containment Targets

N/A

Emerging Platforms

Market Watch - OSSIM

Implications and Dependencies

- Costs and implementation considerations can be substantial (~$30,000 - $150,000).

Roadmap Notes

- OSSIM – Low cost, fully functional Open source product for medium (1,000 units) and small enterprises.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Confidentiality and Integrity

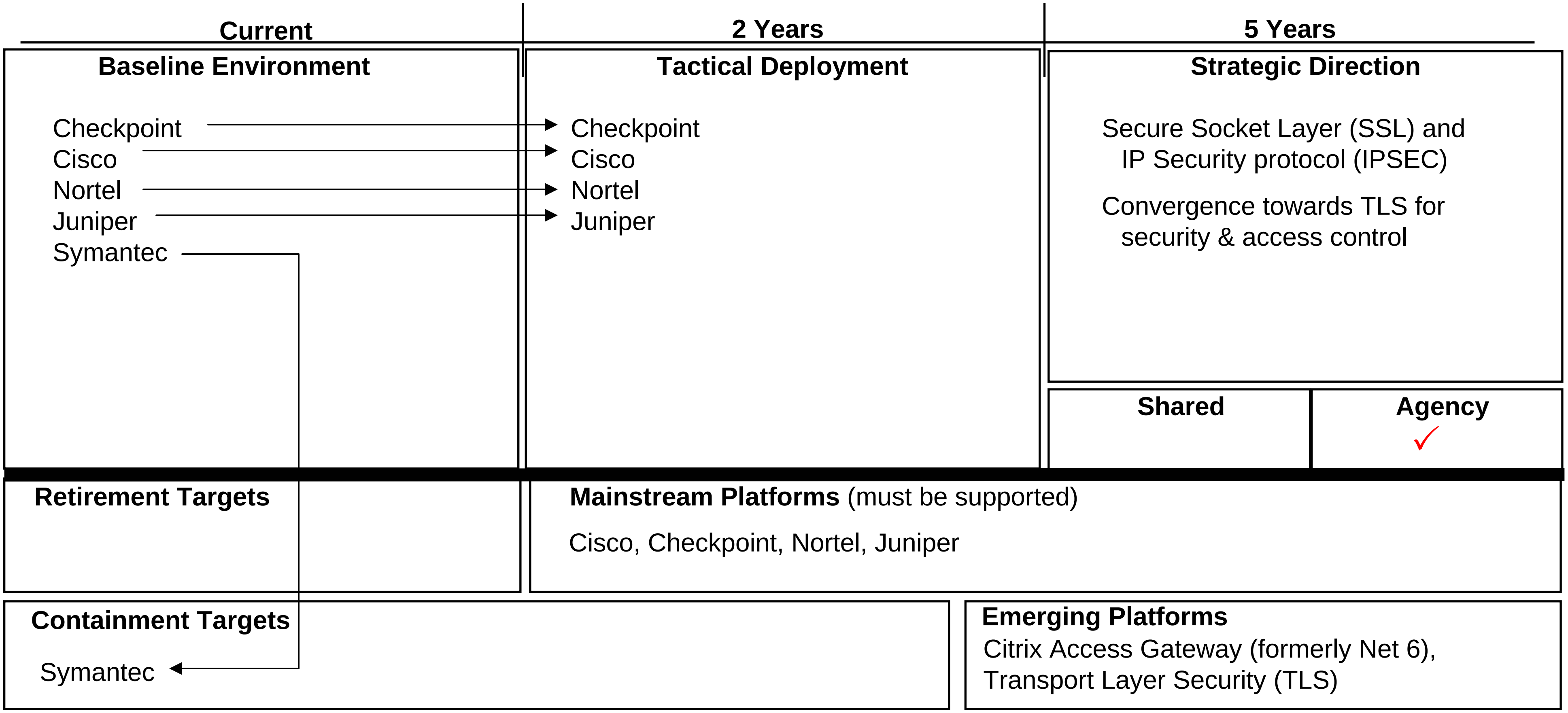
Discipline Roadmap for: SIEM (Security Information & Event Management)

- **Discipline Boundaries:**
  - ❑ SIEM technology is composed of two basic capabilities: Security Information Management (SIM) and Security Event Management (SEM). SIM provides data analysis and reporting of historical events, often used to support regulatory requirements. SEM provides real-time data collection and correlation, often used to support incident response capabilities.
- **Discipline Standards:**
  - ❑ Currently, there are no SIEM specific standards.
- **Migration Considerations:**
  - ❑ None
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ The South Carolina Information and Analysis Center (SC-ISAC) is an education and awareness initiative, jointly developed by the SC Joint Terrorism Task Force (JTTF), the State's Chief Information Office (CIO), the Federal Bureau of Investigation (FBI), and the US Secret Service (USSS). SC-ISAC's mission is to protect the State's citizenry and economy by safeguarding its critical information infrastructure. To that end, SC-ISAC offers a number of security services, including incident response and reporting. Therefore, State Agencies should contact SC-ISAC to develop an integrated incident response plan. Detailed information concerning SC-ISAC can be found on the WWW at http://secure.sc.gov, or by contacting the CIO's Director of Security Policy and Assessment at (803) 896-1660.
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Virtual Private Networks

DOMAIN: SECURITY



Current

Baseline Environment

Checkpoint
Cisco
Nortel
Juniper
Symantec

2 Years

Tactical Deployment

Checkpoint
Cisco
Nortel
Juniper

5 Years

Strategic Direction

Secure Socket Layer (SSL) and IP Security protocol (IPSEC)

Convergence towards TLS for security & access control

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

Cisco, Checkpoint, Nortel, Juniper

Containment Targets

Symantec

Emerging Platforms

Citrix Access Gateway (formerly Net 6), Transport Layer Security (TLS)

Implications and Dependencies

IPSEC often has network traversal vulnerabilities & therefore needs to be secured at the termination point with sufficient IDS capabilities.

Roadmap Notes

These recommendations are valid for IPSEC and SSL implementations.

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Virtual Private Networks

- **Discipline Boundaries:**
  - Virtual Private Networks (VPN) are used to allow mobile users access to the corporate network from home or while they are traveling. Access is encrypted and controlled allowing only authorized users access to authorized resources.
  -
- **Discipline Standards:**
- **Migration Considerations:**
- **Exception Considerations:**
- **Miscellaneous Notes:**
- **Established**
  - August 25, 2004
- **Date Last Updated:**
  - August 23, 2006
- **Next Review Date:**
  - August 2007

State Information Technology Security Policy

1. PURPOSE

To establish a statewide security policy for the protection of Information Technology (IT) assets and resources for the State of South Carolina.

2. SCOPE

This Policy applies to agencies, departments, commissions, and boards (herein referred to as "agencies") that receive, expend or disburse State funds or incur obligations for the State. This policy does not apply to colleges and universities. However, they are encouraged to comply due to the frequent need to access and exchange data with the agencies.

The agency's assigned Designated Approving Authority (DAA), working in conjunction with the Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of statewide information technology policies, standards, and procedures within each agency.

3. POLICY

The State of South Carolina shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

3.1. The policy establishes that:

- Agencies are responsible for providing security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either 1) information collected or maintained by or on behalf of the Agency or 2) information systems used by an Agency or by a contractor of an Agency or other organization on behalf of the Agency.
- Agencies shall ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- Agencies shall ensure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in Agency software application systems.
- Levels of security applied to information systems and resources shall be commensurate with the value of the information being protected.
- Security controls applied to information systems and resources shall be sufficient to contain risk of loss or misuse of the information.
- Agencies are responsible for ensuring that information security management processes are integrated with Agency strategic and operational planning processes.

- Security architecture shall be based on industry-wide, open standards, and where possible, accommodate varying levels of security.
- Inter-Agency IT security components protecting critical Agency and State systems must be interoperable.
- Agencies are responsible for ensuring that staff is adequately trained in information security awareness.

3.2. Each Agency will have a comprehensive, documented set of policies that are periodically reviewed and updated. These policies address key security topic areas, including:

- Security strategy and management
- Security risk management
- Physical security
- System and network management
- System administration tools
- Monitoring and auditing
- Authentication and authorization
- Vulnerability management
- Encryption
- Security architecture and design
- Incident management
- Staff security practices
- Applicable laws and regulations
- Awareness and training
- Collaborative information security
- Contingency planning and disaster recovery

3.3. Agency shall assess their Technology Security by:

- Utilizing self assessments that adhere to industry-accepted best practices.
- Web-based reviews are offered by the CIO to ensure Agency compliance with best practices. Data from these reviews will be warehoused and accessible at the CIO.

Incident Management Best Practice

1. **PURPOSE**

   This policy defines agency responsibilities for responding to and reporting cyber intrusion and for sharing information related to potential incidents or threats with the South Carolina Information Sharing and Analysis Center (SC ISAC).

2. **SCOPE**

   This Policy applies to agencies, departments, commissions, and boards (herein referred to as "agencies") that receive, expend or disburse State funds or incur obligations for the State. This policy does not apply to colleges and universities. However, they are encouraged to comply due to the frequent need to access and exchange data with the agencies.

3. **POLICY**

   To secure and protect the South Carolina's critical information technology (IT) business processes and assets from cyber-crime or cyber-terrorism, State agencies should report all cyber intrusion to the SC ISAC. The agency's Assigned Designated Approving Authority (DAA), should appoint a coordinator to work with the SC ISAC.

4. **Cyber Intrusion:** Agencies should report any of the following acts by any person who, **without authority** or **acting in excess of authority**:

   - Accesses an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network.
   - Accesses, alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices.
   - Accesses, alters, damages, or destroys any computer application systems, programs, or data.
   - Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network.
   - Denies or causes the denial of IT-related services to any authorized user of those services.
   - Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person.
   - Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.
   - Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, or on behalf of the State, a political subdivision of the State, or a medical institution.

- Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network.
- Makes multiple attempts to access an IT device or network system within a brief period of time.

4.1. **Cyber Intrusion Reporting** – The agency should notify SC ISAC within one hour of detecting the intrusion by whatever means of communication is both available and fastest (i.e., phone, fax, e-mail, courier).

- The following information, at a minimum, is required when reporting intrusions to SC ISAC:

  a. Agency name
  b. The Agency SC ISAC Coordinator's name and phone number
  c. Brief description of intrusion and damages (real or anticipated)

- Whenever possible, the agency should capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder.

4.2. **SC ISAC Incident Report –** After notifying SC ISAC of the intrusion, the agency's coordinator should complete a SC ISAC Incident Report (see Attachment A) available from http://secure.sc.gov/site/Incident%20Reporting.asp. The agency's coordinator completing the report should provide as much detail as possible in the remarks fields and annotate the description of the intrusion with explanatory remarks. As more information becomes available or the situation changes, the agency's coordinator should revise and re-submit the incident report to SC ISAC with a clear date-time stamp.

4.3. **SC ISAC Activity –** Depending on the reported damage from the intrusion, SC ISAC will be in constant contact with the agency's coordinator at the affected agency, CIO, South Carolina Law Enforcement Division (SLED), Attorney General's Office, and other organizations, as necessary, until resolution and recovery efforts are completed.

4.4. **Alert Notifications**

4.4.4. **SC ISAC Responsibilities –** As SC ISAC creates or receives computer security alerts, it should determine whether to send it to "All Agencies" or specific Agencies, or only to specific individuals, depending on the security alert. Each alert should state, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk.

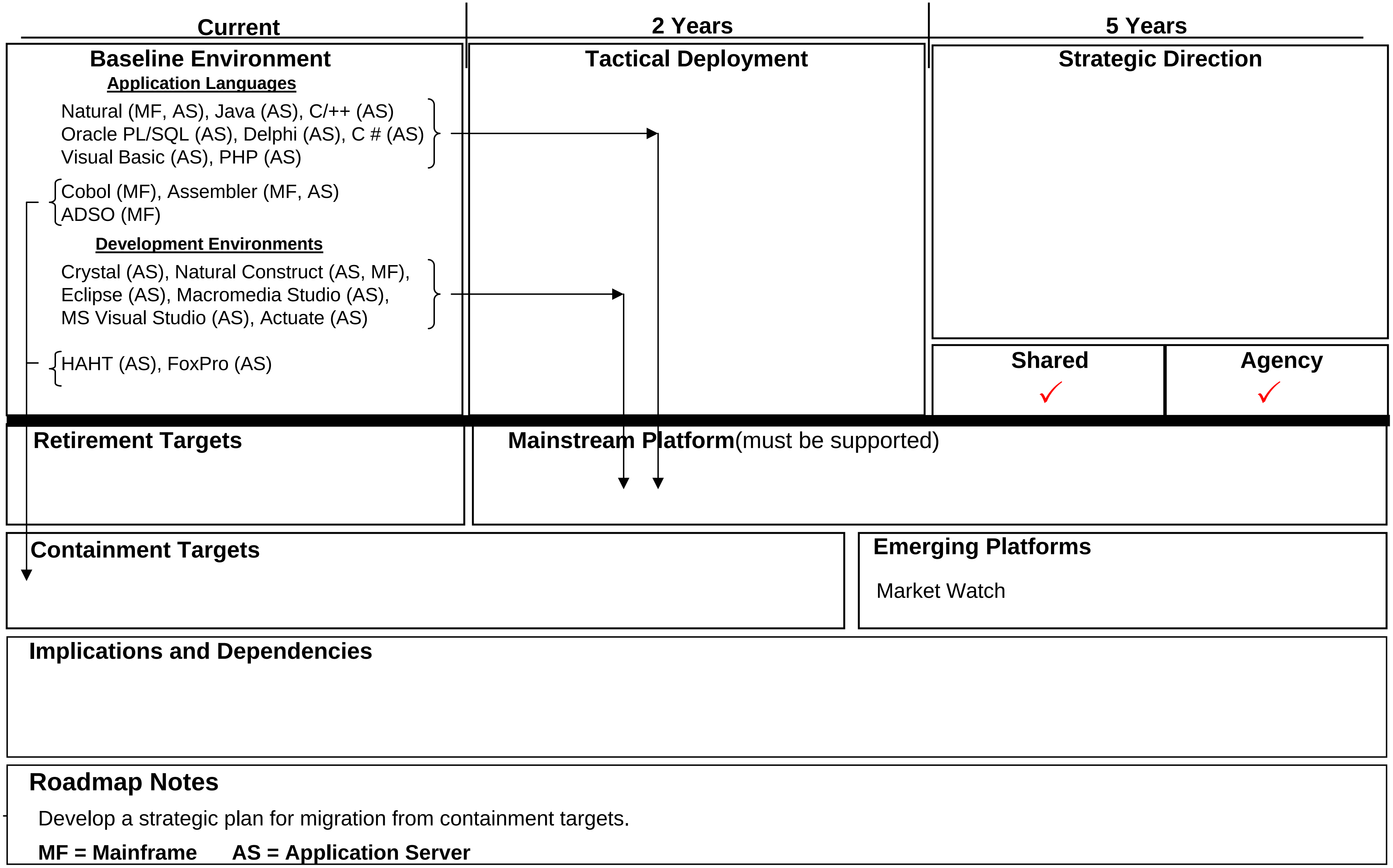
4.4.5. **Agency Responsibilities --** Upon receiving a SC ISAC Alert, agency SC ISAC Coordinators should notify agency personnel about the alert.

4.5. **SC ISAC Membership Form --** Agency SC ISAC Coordinators should complete a SC ISAC Membership Form (see Attachment B) and deliver it to SC ISAC. Agency SC ISAC Coordinators should ensure that the contact information on the form remains current and apprise SC ISAC of any changes.

DISCIPLINE: Application Languages & Development Environments

Discipline Roadmap for: Application Languages & Development Environments

DOMAIN: COMPUTING SERVICES



Current

2 Years

5 Years

Baseline Environment

Application Languages

Natural (MF, AS), Java (AS), C/++ (AS)
Oracle PL/SQL (AS), Delphi (AS), C # (AS)
Visual Basic (AS), PHP (AS)

Cobol (MF), Assembler (MF, AS)
ADSO (MF)

Development Environments

Crystal (AS), Natural Construct (AS, MF),
Eclipse (AS), Macromedia Studio (AS),
MS Visual Studio (AS), Actuate (AS)

HAHT (AS), FoxPro (AS)

Tactical Deployment

Strategic Direction

Shared	**Agency**
✓	✓

Retirement Targets

Mainstream Platform(must be supported)

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Roadmap Notes

Develop a strategic plan for migration from containment targets.

MF = Mainframe **AS = Application Server**

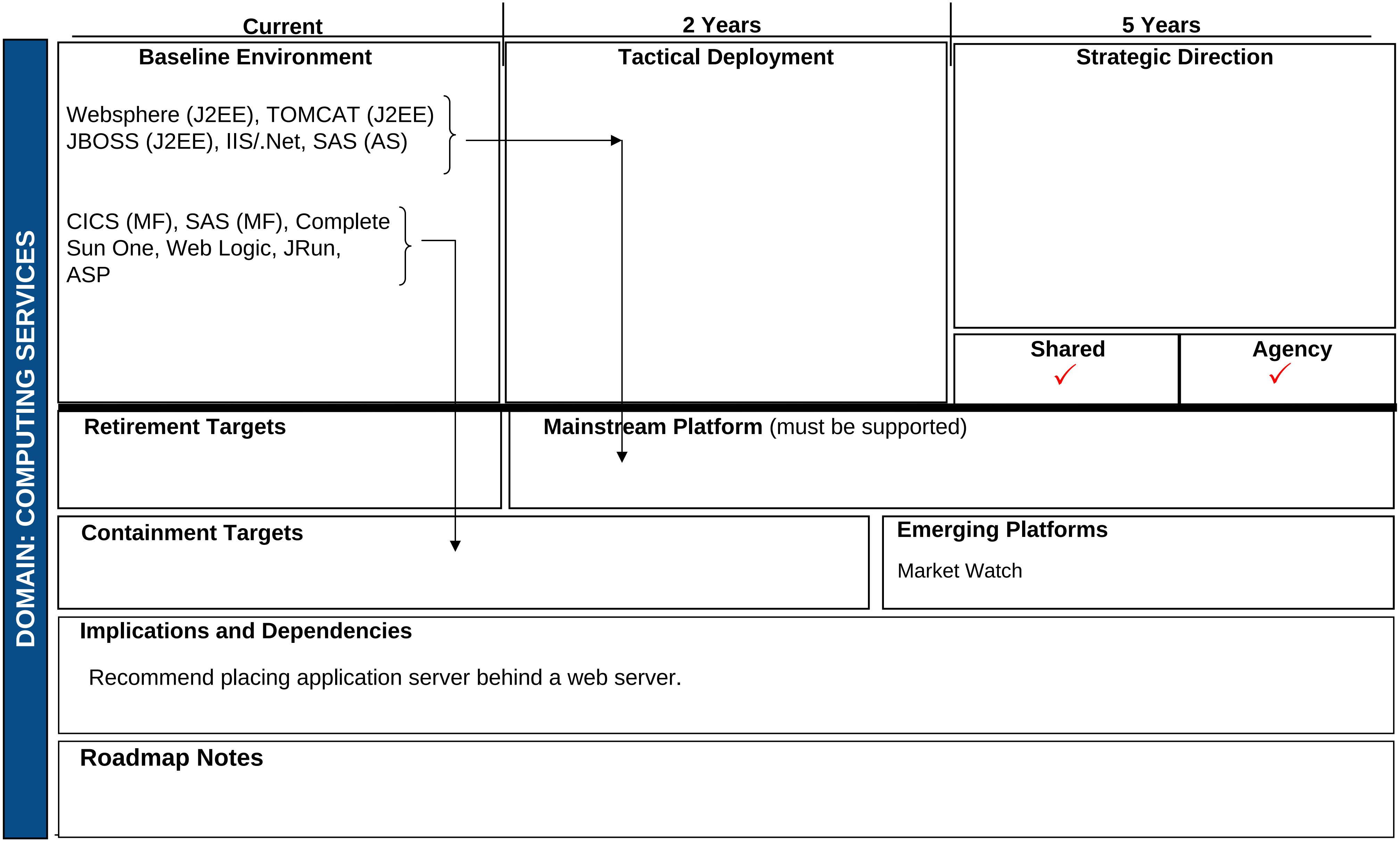
DISCIPLINE: Application Languages & Development Environments

Discipline Roadmap for: Application Languages & Development Environments

- **Discipline Boundaries:**
  - ❑ The structure of this discipline is intended to serve as part of a Service Oriented Architecture approach.
- **Discipline Standards:**
  - ❑ Stay within supported software levels.
- **Migration Considerations:**
  - ❑ Business Case Analysis needed on an agency-by-agency basis when migrating.
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ June 23, 2004
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Application Software Server Environments

Discipline Roadmap for: Application Software Server Environments



DOMAIN: COMPUTING SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Websphere (J2EE), TOMCAT (J2EE) JBOSS (J2EE), IIS/.Net, SAS (AS) CICS (MF), SAS (MF), Complete Sun One, Web Logic, JRun, ASP		
		Shared ✓ / **Agency** ✓

Retirement Targets

Mainstream Platform (must be supported)

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Recommend placing application server behind a web server.

Roadmap Notes

DISCIPLINE: Application Software Server Environments

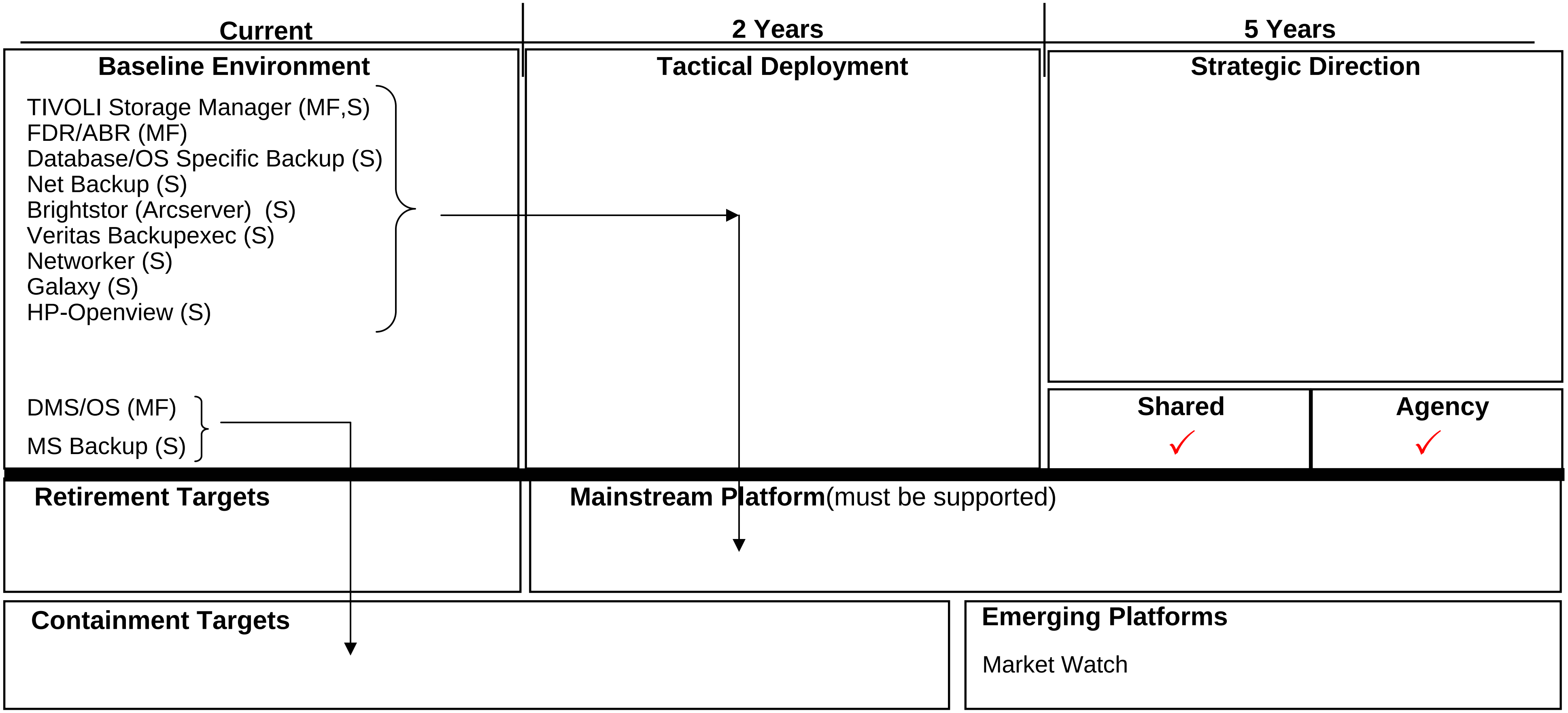
Discipline Roadmap for: Application Software Server Environments

- **Discipline Boundaries:**
  - ❑ The structure of this discipline is intended to serve as part of a Service Oriented Architecture approach.
- **Discipline Standards:**
  - ❑ Stay within supported software levels.
- **Migration Considerations:**
  - ❑ Business Case Analysis needed on an agency-by-agency basis when migrating.
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ June 2004
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Data Backup/Archival

Discipline Roadmap for: Data Backup/Archival

DOMAIN: COMPUTING SERVICES



Current

Baseline Environment

TIVOLI Storage Manager (MF,S)
FDR/ABR (MF)
Database/OS Specific Backup (S)
Net Backup (S)
Brightstor (Arcserver) (S)
Veritas Backupexec (S)
Networker (S)
Galaxy (S)
HP-Openview (S)

DMS/OS (MF)
MS Backup (S)

2 Years

Tactical Deployment

5 Years

Strategic Direction

Shared ✓

Agency ✓

Retirement Targets

Mainstream Platform(must be supported)

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Pirmary hardware/software configuration must be available on all recovery systems at the same or higher releases.

Roadmap Notes

MF – Mainframe, S – Server. Develop a 5 year strategic plan, AOC Phase II.

DISCIPLINE: Data Backup/Archival

Discipline Roadmap for: Data Backup/Archival

- **Discipline Boundaries:**
  - ❑ Data Backup and archival software/methodology for mainframe and/or server platforms.
- **Discipline Standards:**
  - ❑ Must meet average recovery time requirements as per agency Disaster Recovery Plan.
- **Migration Considerations:**
  - ❑ How to handle older data backup/recovery media/software when converting to newer technology.
- **Exception Considerations:**
  - ❑ None
- **Miscellaneous Notes:**
  - ❑ None
- **Established Date:**
  - ❑ February 2006
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Mainframe Hardware and OS

Discipline Roadmap for: Mainframe Hardware and OS

DOMAIN: COMPUTING SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
DEC Alpha 2100 4/200 OpenVMS DEC Alpha 4000 Open VMS 7.2-1 Unisys/ClearPath → IBM Z800-Z0S →	“Z” Series/ZOS	

Shared	**Agency**
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

ZOS, “Z” Series

Containment Targets

DEC Alpha, Open VMS, Unisys/ClearPath

Emerging Platforms

IFL (Linux)

Implications and Dependencies

DEC Alpha needs to be retired. Need retirement plan and date. Open VMS needs to be replaced.

Roadmap Notes

Need to form a work group to develop an Open VMS/Unisys/DEC migration strategy.

DISCIPLINE: Mainframe Hardware and OS (Cont'd)

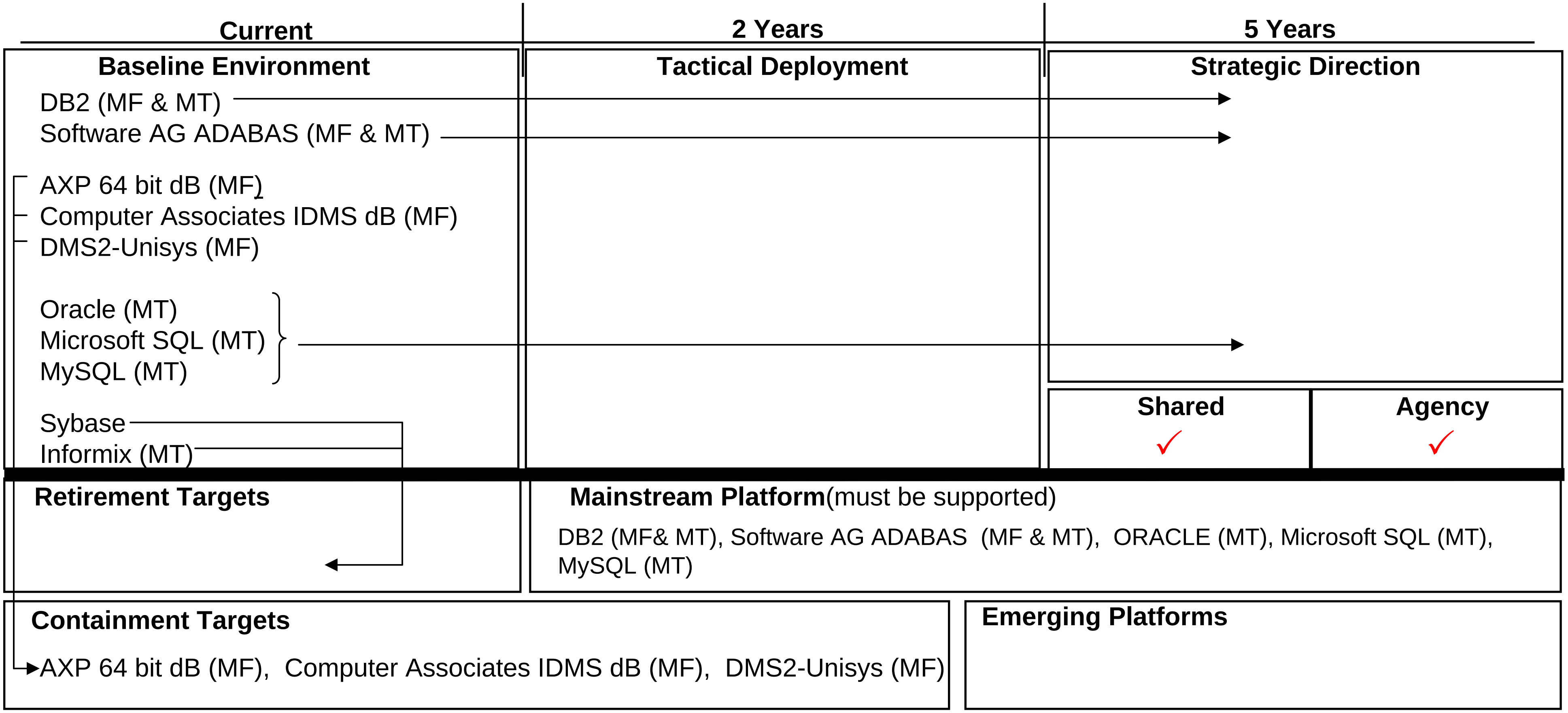
Discipline Roadmap for: Mainframe Hardware and OS

- **Discipline Boundaries:**
  - ❑ None.
- **Discipline Standards:**
  - ❑ None.
- **Migration Considerations:**
  - ❑ Open VMS-Need a migration strategy for each application. Planning should begin now.
  - ❑ The transition from OS/390 will be completed by 12/2005.
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ Linux on the IFL needs to be evaluated.
- **Established Date:**
  - ❑ October 7, 2003
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Mainframe & Mid-Tier Databases

Discipline Roadmap for: Mainframe(MF) & Mid-Tier(MT) Databases

DOMAIN: COMPUTING SERVICES



Current | 2 Years | 5 Years

Baseline Environment

DB2 (MF & MT)
Software AG ADABAS (MF & MT)

AXP 64 bit dB (MF)
Computer Associates IDMS dB (MF)
DMS2-Unisys (MF)

Oracle (MT)
Microsoft SQL (MT)
MySQL (MT)

Sybase
Informix (MT)

Tactical Deployment

Strategic Direction

Shared ✓

Agency ✓

Retirement Targets

Mainstream Platform(must be supported)

DB2 (MF& MT), Software AG ADABAS (MF & MT), ORACLE (MT), Microsoft SQL (MT), MySQL (MT)

Containment Targets

AXP 64 bit dB (MF), Computer Associates IDMS dB (MF), DMS2-Unisys (MF)

Emerging Platforms

Implications and Dependencies

Any decision involving VAX/VMS must also take into account AXP 64 dB, and vice-versa.

Similarly, any decision involving a Unisys platform must include a decision for the disposition of DMS2.

Roadmap Notes

DISCIPLINE: Mainframe & Mid-Tier Databases (Cont'd)

Discipline Roadmap for: Mainframe(MF) & Mid-Tier(MT) Databases

- **Discipline Boundaries:**
  - The structure of this discipline is intended to serve as part of a Service Oriented Architecture approach.
- **Discipline Standards:**
  - None.
- **Migration Considerations:**
  - None.
- **Exception Considerations:**
  - None.
- **Miscellaneous Notes:**
  - Need to research the prevalence/importance of Oracle in this context.
- **Established Date:**
  - June 23, 2004
- **Date Last Updated:**
  - June 28, 2006
- **Next Review Date:**
  - June 2007

DISCIPLINE: Mainframe & Server Middleware

Discipline Roadmap for: Mainframe & Server Middleware

DOMAIN: COMPUTING SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

Baseline Environment

Entire X
DB2 Connect
SQL Gateway
COM/DCOM
RPC
EDI
Web Services
Attunity

Tactical Deployment

Strategic Direction

Market Watch

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

Containment Targets

Emerging Platforms
Market Watch

Implications and Dependencies

Roadmap Notes

DISCIPLINE: Mainframe & Server Middleware

Discipline Roadmap for: Mainframe & Server Middleware

- **Discipline Boundaries:**
- **Discipline Standards:**
  - ❑ Current within 1 release of mainstream software.
- **Migration Considerations:**
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ January 25, 2006
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Service & Data Layer Servers - Hardware

Discipline Roadmap : Service & Data Layer Servers - Hardware

DOMAIN: COMPUTING SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
RISC → INTEL Compatible →		Market Watch AMD

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

RISC, Intel Compatible

Containment Targets

Emerging Platforms

Implications and Dependencies

Roadmap Notes

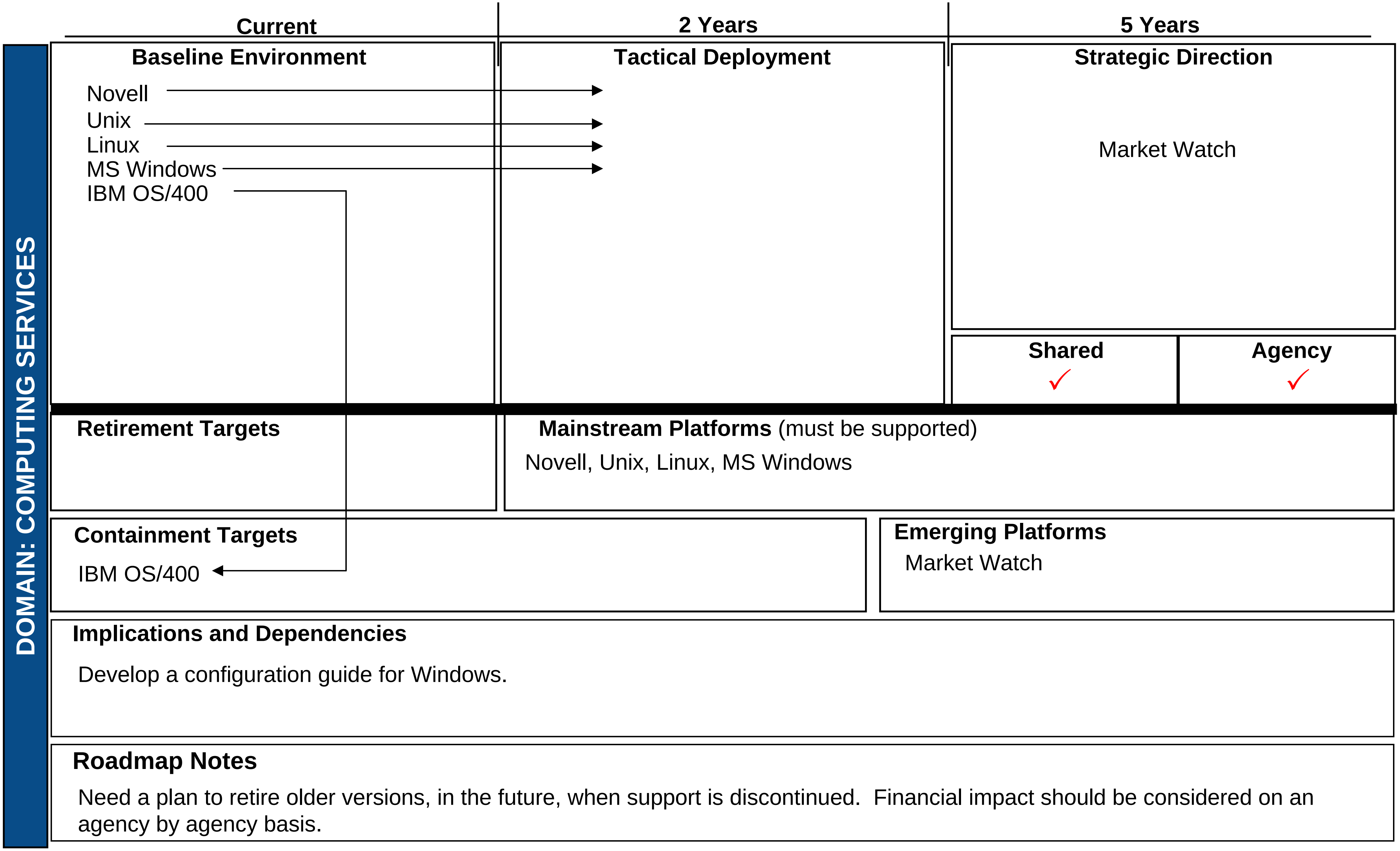
DISCIPLINE: Service & Data Layer Servers - Hardware

Discipline Roadmap for: Service & Data Layer Servers - Hardware

- **Discipline Boundaries:**
  - ❑ Application and data services for small to mid-range servers not including mainframes.
- **Discipline Standards:**
  - ❑ None.
- **Migration Considerations:**
  - ❑ None.
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ November 2004
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Service & Data Layer Servers – OS

Discipline Roadmap for: Service & Data Layer Servers – OS



DOMAIN: COMPUTING SERVICES

Current | 2 Years | 5 Years

Baseline Environment

Novell
Unix
Linux
MS Windows
IBM OS/400

Tactical Deployment

Strategic Direction

Market Watch

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

Novell, Unix, Linux, MS Windows

Containment Targets

IBM OS/400

Emerging Platforms

Market Watch

Implications and Dependencies

Develop a configuration guide for Windows.

Roadmap Notes

Need a plan to retire older versions, in the future, when support is discontinued. Financial impact should be considered on an agency by agency basis.

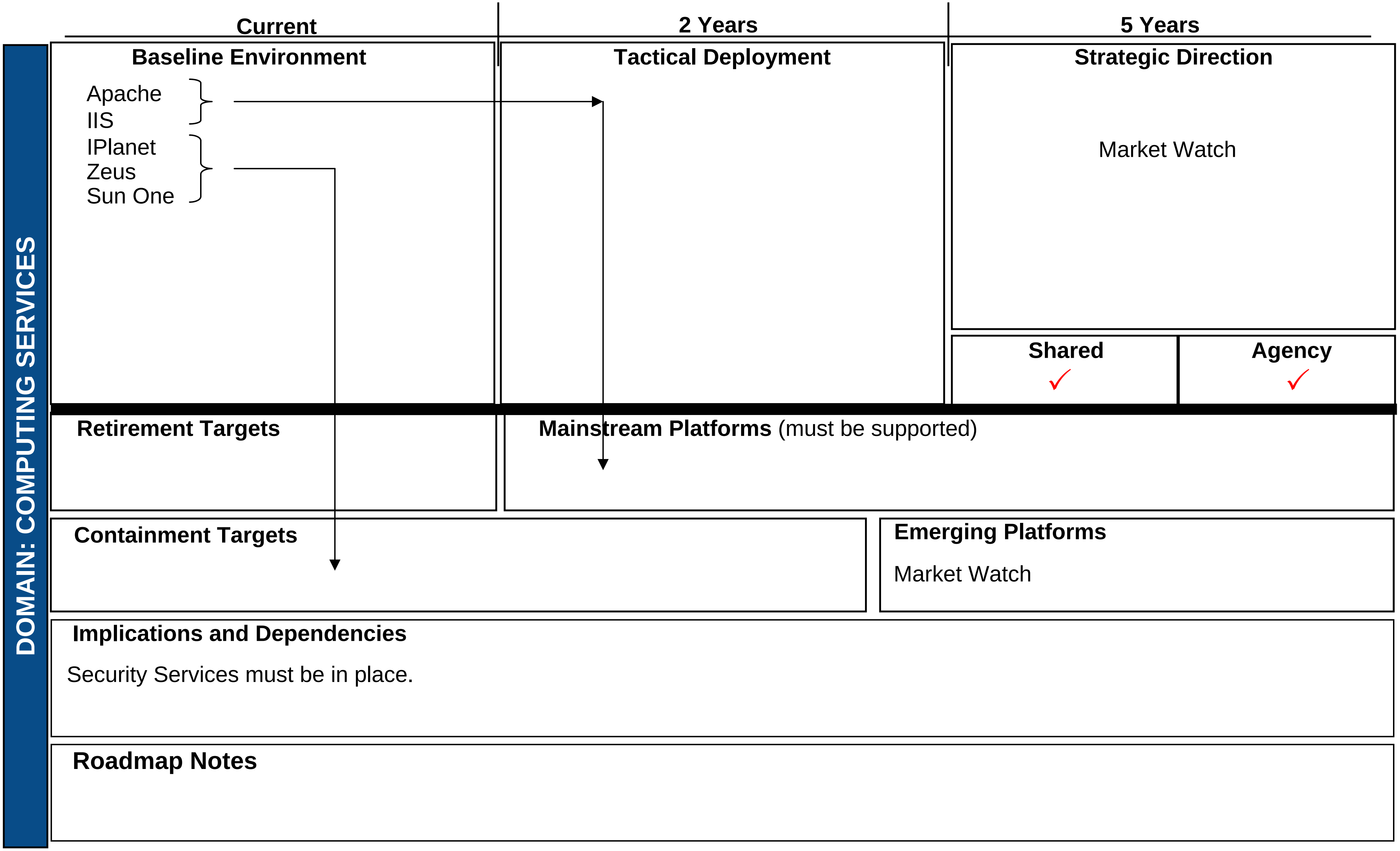
DISCIPLINE: Service & Data Layer Servers – OS

Discipline Roadmap for: Service & Data Layer Servers – OS

- **Discipline Boundaries:**
  - ❑ Application and data services for small to mid-range servers not including mainframes.
- **Discipline Standards:**
  - ❑ No more than 1 release behind current standard releases.
- **Migration Considerations:**
  - ❑ MS Windows 2000 migration strategy needed
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ November 2004
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: WEB SERVER SOFTWARE

Discipline Roadmap for: Web Server Software



DOMAIN: COMPUTING SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Apache IIS IPlanet Zeus Sun One		Market Watch

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Security Services must be in place.

Roadmap Notes

DISCIPLINE: Web Server Software

Discipline Roadmap for: Web Server Software

- **Discipline Boundaries:**
  - ❑ Intranet and Internet Servers
- **Discipline Standards:**
  - ❑ Stay within supported software levels
- **Migration Considerations:**
  - ❑ Migrate when usage of product becomes less than 1% of market share
- **Exception Considerations:**
  - ❑ None.
- **Miscellaneous Notes:**
  - ❑ None.
- **Established Date:**
  - ❑ January 25, 2006
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Storage Subsystem - Disk

Discipline Roadmap for: Storage Subsystem - Disk

DOMAIN: COMPUTING SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
RAID 5 RAID 0 RAID 1 SAN Storage Area Network NAS Net Attached Storage Internal Drive Optical CD DVD		

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platform(must be supported)

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Long range Strategic Direction should include RAID 5 and SAN. Caution should be used when utilizing RAID 0 due to the potential for full volume loss.

Roadmap Notes

Develop guidelines and usage strategy for each technology.

DISCIPLINE: Storage Subsystem - Disk

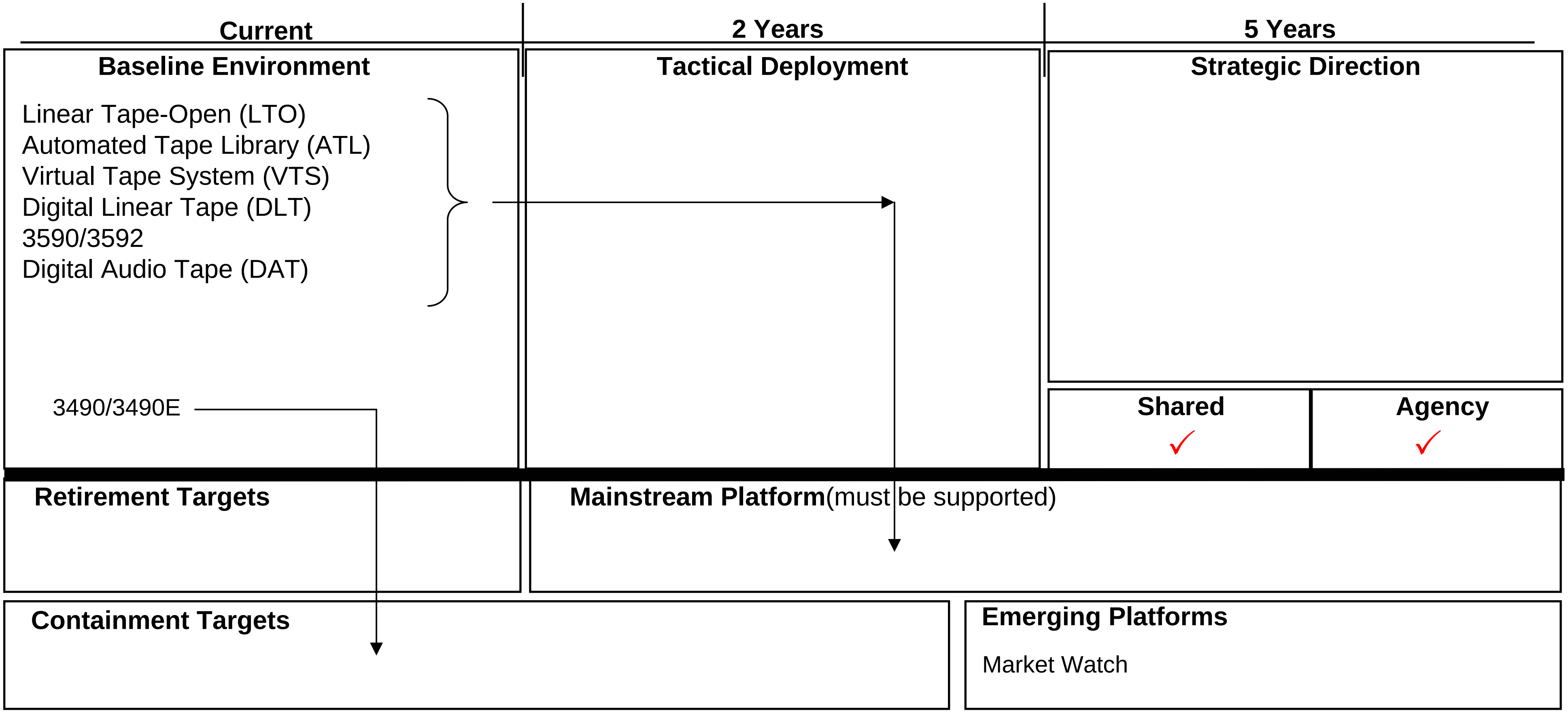
Discipline Roadmap for: Storage Subsystem - Disk

- **Discipline Boundaries:**
  - ❑ Disk storage for mainframe and/or server platforms.
- **Discipline Standards:**
  - ❑ None
- **Migration Considerations:**
  - ❑ Evaluate storage capacity and future growth for migration strategies.
- **Exception Considerations:**
  - ❑ None
- **Miscellaneous Notes:**
  - ❑ None
- **Established Date:**
  - ❑ February 2006
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Storage Subsystem - Tape

Discipline Roadmap for: Storage Subsystem - Tape

DOMAIN: COMPUTING SERVICES



Current | 2 Years | 5 Years

Baseline Environment

Linear Tape-Open (LTO)
Automated Tape Library (ATL)
Virtual Tape System (VTS)
Digital Linear Tape (DLT)
3590/3592
Digital Audio Tape (DAT)

3490/3490E

Tactical Deployment

Strategic Direction

Shared ✓

Agency ✓

Retirement Targets

Mainstream Platform(must be supported)

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Roadmap Notes

Develop guidelines and usage strategy for each technology.

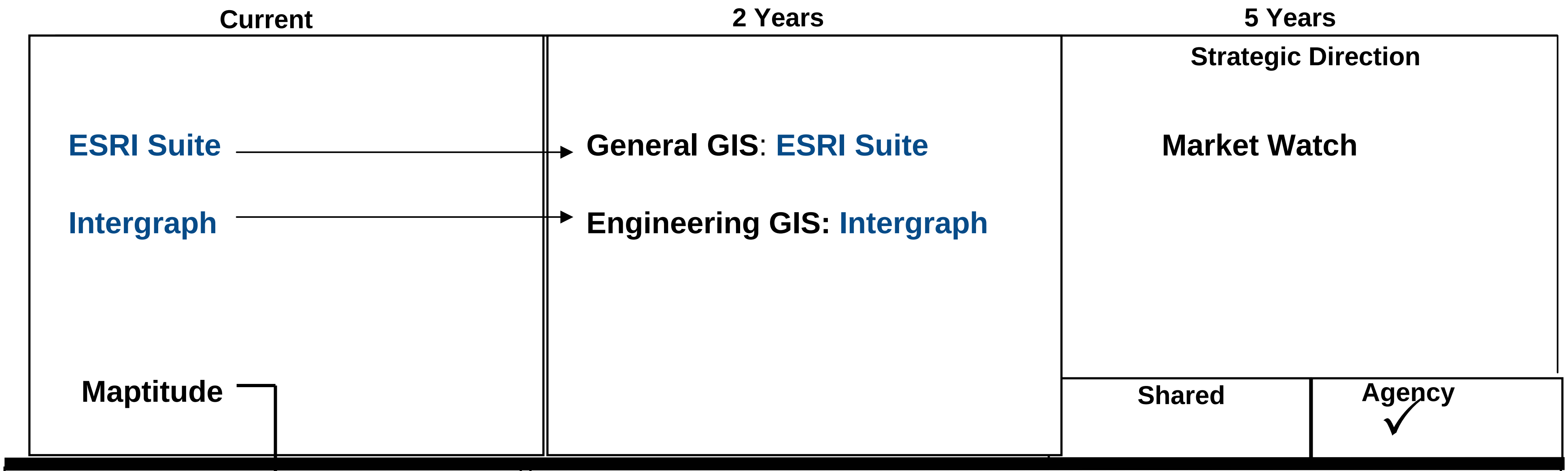
DISCIPLINE: Storage Subsystem - Tape

Discipline Roadmap for: Storage Subsystem - Tape

- **Discipline Boundaries:**
  - ❑ Tape storage for mainframe and/or server platforms.
- **Discipline Standards:**
  - ❑ None
- **Migration Considerations:**
  - ❑ Evaluate storage capacity and future growth for migration strategies.
- **Exception Considerations:**
  - ❑ None
- **Miscellaneous Notes:**
  - ❑ None
- **Established Date:**
  - ❑ February, 2006
- **Date Last Updated:**
  - ❑ June 28, 2006
- **Next Review Date:**
  - ❑ June 2007

DISCIPLINE: Geographic Information Systems (GIS)

Discipline Roadmap for: Geographic Information Systems (GIS)



Current

ESRI Suite

Intergraph

Maptitude

2 Years

General GIS: **ESRI Suite**

Engineering GIS: Intergraph

5 Years

Strategic Direction

Market Watch

Shared

Agency ✓

Retirement Targets

Mainstream Platforms (must be supported)

ESRI, Intergraph

Containment Targets

Maptitude (runs on Windows XP & 2000 OS)

Emerging Platforms

Implications and Dependencies

- GPS-Transfer standards to ESRI and Intergraph such as Trimble & Magellan (Thales Navigation)
- ERDAS Imagine image classification system and Image/Stereo Analyst for image integration in ArcGIS

Roadmap Notes

- Need state GIS coordinator, creation/empowerment of GIS Coordination Council, implementation of GIS plan**.**

DISCIPLINE: Geographic Information Systems (Cont'd)

Discipline Roadmap for: Geographic Information Systems (GIS)

- **Discipline Boundaries:**
  - GPS is included in this discipline only to the extent that GPS devices have the capability of exporting data accurately to ESRI and INTERGRAPH application suites.
- **Discipline Standards:**
  - Federal Geographic Data Committee (FGDC) and other applicable data standards
  - ESRI, Intergraph
- **Migration Considerations:**
  - Costs, Data/record formats and compatibility
- **Exception Considerations:**
  - <Add text>
- **Miscellaneous Notes:**
  - The GIS PlanGraphics Reports (Volume 1 and Volume 2) dated 4/30/2001 and preceding needs analysis have been obtained (SEE:http://www.scgs.state.sc.us/smac/default.htm**).**
- **Established Date:**
  - November 19, 2003
- **Date Last Updated:**
  - September 27, 2006
- **Next Review Date:**
  - September 2007

DISCIPLINE: CRM

Discipline Roadmap for: CRM (Customer Relationship Management)

DOMAIN: Enterprise Applications

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Agency Proprietary Systems	SAP	Market Watch

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

SAP

Containment Targets

Emerging Platforms

Market Watch

Implications and Dependencies

Pending SCEIS (SAP) human resource and finance implementation.

Roadmap Notes

DISCIPLINE: CRM

Discipline Roadmap for: CRM (Customer Relationship Management)

- **Discipline Boundaries:**
  - ❑ CRM is a systematic strategy for utilizing customer information and customer contact history to enhance customer experience and influence future behavior. CRM is not solely an information technology solution but an holistic approach to managing customer relations.
- **Discipline Standards:**
  - ❑ There are no CRM standards, per se, so agencies should focus on interoperability and underlying infrastructure standards, e.g. XML and W3C. The market leaders as identified by Gartner's magic quadrant are: IBM Business Consulting Services, Accenture, and Deloitte
- **Migration Considerations:**
  - ❑
- **Exception Considerations:**
  - ❑
- **Miscellaneous Notes:**
  - ❑
- **Established**
  - ❑ September 27, 2006
- **Date Last Updated:**
  - ❑ September 27, 2006
- **Next Review Date:**
  - ❑ September 2007

DISCIPLINE: Enterprise Resource Planning (ERP)

Discipline Roadmap for: Enterprise Resource Planning (ERP)

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
SAP STARS STATEWIDE PAYROLL SYSTEM HRIS APSC Multiple agency level accounting, human resources, and payroll systems and subsystems	SAP (ERP 2004) STATEWIDE PAYROLL SYSTEM HRIS	SAP Shared ✓ **Agency**

Retirement Targets

Mainstream Platforms (must be supported)

STATEWIDE PAYROLL SYSTEM, HRIS, SAP

Containment Targets

Multiple agency level accounting, human resources, and payroll systems and subsystems should be contained. Stars and APSC should be contained as they will be replaced in 2007.

Emerging Platforms

SAP

Implications and Dependencies

- **Currently there are 173 different Applications in 70 different agencies.**
- **All agency-wide accounting,procurement, HR budget and payroll systems except for SAP should be contained.**

Roadmap Notes: Implementation of SAP is dependent upon availability of adequate funding and central support.

DISCIPLINE: Enterprise Resource Planning (Cont’d)

Discipline Roadmap for: Enterprise Resource Planning (ERP)

- **Discipline Boundaries:**
  - ❑ “Back office” components of SAP software (e.g. finance, procurement, budget, HR, payroll, supplier relationship management, etc.)
- **Discipline Standards:**
  - ❑ SAP
- **Migration Considerations:**
  - ❑ A statewide rollout plan was developed as part of the SCEIS financial and procurement blueprint. This Plan will be managed and updated periodically by the SCEIS Executive Oversight Committee to contain the number of rollouts and to accommodate agencies with aging systems. The initial realization phase began in August 2006 for the Budget and Control Board, State Treasurer’s Office, Comptroller General’s Office, Office of Regulatory Staff, Department of Mental Health and the BARS agencies and will continue for the remaining 60 state agencies over a four year period.
- **Exception Considerations:**
  - ❑ None
- **Miscellaneous Notes:**
  - ❑ The SCEIS Executive Oversight Committee (decision making body), the Technical Services Advisory Committee and a SCEIS Users Group have been established and will review issues and update the Enterprise Applications Domain Subcommittee, on a periodic basis.
- **Established Date:**
  - ❑ November 19, 2004
- **Date Last Updated:**
  - ❑ September 27, 2006
- **Next Review Date:**
  - ❑ September 2007

DISCIPLINE: BI

Discipline Roadmap for: BI (Business Intelligence)

DOMAIN: Enterprise Applications

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
SAS Clementine Agency Specific Applications, Data Warehouses, and Data Marts	SAP SAS Clementine	Market Watch

Shared	Agency
✓	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

Business Intelligence systems are generally built on a database platform, but structured for online analytical processing (OLAP) rather than online transactional processing (OLTP). The database platforms should conform to established standards, please reference the Computing Services Domain Mainframe & Mid-tier Databases for a complete list.

Roadmap Notes

Current BI activity is agency-specific. Future vision should include enterprise BI across agencies. BI systems must be differentiated from agency and enterprise operational systems.

DISCIPLINE: BI

Discipline Roadmap for: BI (Business Intelligence)

- **Discipline Boundaries:**
  - ❑ BI software and systems, including integration with databases and data warehouses. This includes selecting, blueprinting, gathering requirements, designing and rolling out solutions to end-users.
- **Discipline Standards:**
  - ❑ While there are market leaders and standard techniques for BI analytical processing, such as the OLAP cube, the only applicable standards are those for the underlying database management system.
- **Migration Considerations:**
  - ❑ N/A
- **Exception Considerations:**
  - ❑ Agency specific applications should be considered on a case by case basis.
- **Miscellaneous Notes:**
  - ❑ Today's business decision-making is increasingly dependent on Business Intelligence systems.
- **Established**
  - ❑ September 26, 2006
- **Date Last Updated:**
  - ❑ September 26, 2006
- **Next Review Date:**
  - ❑ September 2007

DISCIPLINE: Web Commerce

Discipline Roadmap for: Web Commerce

Current	2 Years	5 Years
Baseline	**Tactical Deployment**	**Strategic Direction**
HAHT (CIO) SC.GOV Agency developed applications Microsoft .Net, Websphere FrontPage, DreamWeaver Oracle with PSP SCBOS SSL (Verisign, EnTrust certificates)	W3C Recommendations	Adopt all new W3C recommendations as developed **Shared** ✓ **Agency** ✓

Retirement Targets

HAHT

Mainstream Platforms (must be supported)

Containment Targets

FrontPage, DreamWeaver for commerce (mainstream for HTML)

Emerging Platforms

Market Watch

Implications and Dependencies

The growth of Enterprise applications for state e-commerce must be encouraged.

Security and privacy of customer/citizen information are of the highest priority.

Roadmap Notes

The Committee endorses the W3C recommendations found at http://www.w3.org/TR/#Recommendations.

DISCIPLINE: Web Commerce

Discipline Roadmap for: Web Commerce

- **Discipline Boundaries:**
  - Web Commerce includes the ability to do business with SC state government and obtain state government products and services over the Internet using a standard interface.
- **Discipline Standards:**
  - State Government entities should utilize the Worldwide Web Consortium Recommendations/Standards http://www.w3.org/TR/#Recommendations.
- **Migration Considerations:**
  - HAHT applications must be replaced by standard platform applications.
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - The State must present a unified, easy to navigate face to citizens and to businesses.
  - Examples of Web Commerce engines meeting standards include SC.GOV, SCBOS, and SCEIS.
- **Established Date:**
  - September 27, 2006
- **Last Review Date:**
  - September 27, 2006
- **Next Review Date:**
  - September 2007

DISCIPLINE: Electronic Document Management Systems

Discipline Roadmap for: EDMS

Current

See attached survey completed in July 2004.

2 Years

Agencies should select products to meet business needs following the recommendations referenced in the Roadmap notes.

5 Years

Strategic Direction

Market Watch

Shared	Agency
	✓

Retirement Targets

None

Mainstream Platforms (must be supported)

Not applicable

Containment Targets

None

Emerging Platforms

Market Watch

Implications and Dependencies

- There will continue to be multiple EDMS products used by state agencies.
- The general recommendations from the SC Department of Archives and History (SCDAH) will guide future implementations.

Roadmap Notes

- The Committee endorses the basic recommendations from the SCDAH in its documents entitled "Electronic Document Management Systems" (Feb. 2005 Version 1) and "Digital Imaging" (Feb. 2005, Version 1) .

DISCIPLINE: Electronic Document Management Systems

Discipline Roadmap for: EDMS

- **Discipline Boundaries:**
  - EDMS includes document management, imaging, workflow, text retrieval, and records management.
- **Discipline Standards:**
  - See Roadmap notes
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - The SCDAH will continue to update the referenced documents based upon input from participating state agencies and industry associations, particularly the Association for Information and Image Management International (AIIM).
- **Established Date Last Updated:**
  - March 23, 2005
- **Date Last Reviewed:**
  - September 27, 2006
- **Next Review Date:**
  - September 2007

DISCIPLINE: Asset Management

Discipline Roadmap for: Asset Management

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current	2 Years	5 Years

Baseline Environment

No Baseline

Known products in use

- Microsoft System Management Server
- SAMS (Agency Management System)
- Administrative Information Management System (AIMS—old Oracle tool)
- Zenworks Asset Management
- Altiris Asset Management
- Tivoli License Manager
- Track-IT
- Access Database
- Spreadsheets

Tactical Deployment

Small Agency(<1K Clients)

Database or Spreadsheet

Medium Agency(>1K and <7K Clients)

Altiris

Large Agency(>3K Clients)

Remedy

Enterprise Solution

Remedy Enterprise

The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for IT Service Support that addresses Asset Management.

Strategic Direction

Market Watch

Market watch of ITIL and best practices for Asset Management.

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

Database, Spreadsheet, Altiris, Remedy, Microsoft SMS

Containment Targets

Zenworks, Tivoli, Track-it

Emerging Platforms

Market Watch

Implications and Dependencies

Any small agency with 1K or less clients would not benefit from an asset management tool (too costly), Gartner suggests using a database or (spreadsheet).

Track-IT does not have API's for integration with other systems, as all functionality is self-contained. Implications – to obtain a hardware/software inventory from an agency using Track-IT would require programming.

Roadmap Notes

. Asset Management is a part of overall IT Service Management best illustrated by the IT Infrastructure Library guides, which is the most widely accepted approach to providing a comprehensive and consistent set of best practices.

DISCIPLINE: Asset Management

Discipline Roadmap for: Asset Management

- **Discipline Boundaries:**
  - This standard applies to Asset Management tools.
- **Discipline Standards:**
  - All end user support tools should aid the organization in adhering to ITIL best practices for Service Delivery and Support.
- **Migration Considerations:**
  - Dependent on the product that data is being migrated to/from. If an API does not exist, migration could be costly. A basic knowledge of ITIL best practices will be required.
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - November 16, 2005
- **Date Last Reviewed:**
  - October 25, 2006
- **Next Review Date:**
  - October 2007

DISCIPLINE: Problem/Change/Configuration Management

Discipline Roadmap for: Problem/Change/Configuration Management

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current	2 Years	5 Years
Baseline Environment Baseline on final slide	**Tactical Deployment** The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for problem, configuration and change management. www.itil.com	**Strategic Direction** Market watch of ITIL and best practices for problem, configuration and change management.

Shared	Agency
☑	☑

Retirement Targets
Independent solutions that only address one of the above processes in a vacuum.

Mainstream Platforms (must be supported)

Supported OSs: Windows, AIX, Novell, Z/OS, UNIX

Containment Targets

DCL, LLR, and Liberium because they are not supported; products designed for DEC, Windows 2000 platforms.

Emerging Platforms

LINUX & Windows

Implications and Dependencies

Management tools must adhere to the hardware and product versions of the AOC standards. A configuration management database (CMDB) should be employed to track problem, configuration and change management.

Roadmap Notes
The ITIL Standards support the AOC recommendations for operating systems. Gartner cites BMC and CA as being leaders in providing solutions for ITIL compliance in problem, configuration, and change management.

DISCIPLINE: Problem/Change/Configuration Management

Discipline Roadmap for: Problem/Change/Configuration Management

- **Discipline Boundaries:**
  - There should be a close interface between the Problem Management, Change Management, and Configuration Management..
  - Change Management: Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.
  - Configuration Management: The process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items and Requests For Change, and verifying the completeness and correctness of Configuration Items.
  - Problem Management:: Process that minimizes the effect on Customer(s) of defects in services and within the infrastructure, human errors and external events.
- **Discipline Minimum Standards:**
  - All tools should support the implementation of the ITIL best practice framework.
  - Information Technology Information Library (ITIL) is a set of best practices used to deliver high quality IT services including problem, configuration and change management. The best practices described in ITIL represent the consensus derived from over a decade of work by thousands of IT and data processing professionals' world-wide, including hundreds of years of collective experience. Because of its depth and breadth, the ITIL has become the defacto world standard for IT best practices.
- **Migration Considerations:**
  - As with adaptation of any new business practices, training will be required.
  - First, a vision has to be created. Next, the IT and business strategies should be aligned. The second step consists of analyzing the organization and its current position. In this step the organization answers the question 'where are we now?' The following step is setting goals and priorities regarding the improvement process. The fourth step is the improvement of the service through ITIL best practices in configuration, problem and change management. The fifth and final step consists of measuring the improvement to examine if processes are enhancing performance.
  - Change management will require baseline analysis of IT operations processes for problem, change and configuration management.
  - A basic knowledge of ITIL best practices will be required.
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - Gartner reports that because of the popularity of process frameworks, such as ITIL, and the desire of IT organizations to cut costs and improve IT service and support, many IT organizations are moving beyond the vendors' traditional incident management ticketing systems to vendors that offer a richer suite of IT service support tools.
- **Established Date**
  - April 27, 2005
- **Date Last Updated:**
  - October 25, 2006
- **Next Review Date:**
  - October 2007

DISCIPLINE: Problem/Change/Configuration Management

Discipline Roadmap for: Problem/Change/Configuration Management

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current Baseline Environment

ACS
CiscoWorks
Envision (Analysis SW)
LAN scan
NetBotz
NetVision (Management Tools)
SMP (MRTG)
SNMP access to servers - OS tools to monitor
ELM Performance Manager 3.0
DS Expert 3.40
DS Analyzer v2.02
NetScan Pro 6.1

Cetus Storm Windows
IBM Director
MRTG
Cisco WAN Mgr
Nortel Optivity
SNMP Utilities
Watchguard Technologies
Bindview RMS 7.2
Whats Up Gold (7.4)
HP Openview
Somix WebNM

DISCIPLINE: Performance Capacity Management Tools

Discipline Roadmap for: Performance Capacity Management Tools

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current	2 Years	5 Years
Baseline Environment Somix WebNM SMS-Desktop MRTG-Bandwidth (Or any MRTG/rrdtool based application) Bindview RMS 7.2 DS Analyzer v2.02	**Tactical Deployment** The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for performance capacity management. www.itil.com	**Strategic Direction** Market Watch of products that enable performance and capacity management by adhering to ITIL best practices for Service Delivery and Support.

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

Somix WebNM, MRTG-Bandwidth

Containment Targets

SMS-Desktop, Bindview RMS 7.2, DS Analyzer v2.02

Emerging Platforms

Implications and Dependencies – Certain open source applications are available alone or as part of a more comprehensive network management application. Because of the inherent nature of open source applications, support and training are limited.

Roadmap Notes – According to Computer World Magazine, more advanced capacity planning software does more than track historical trends. It also lets IT planners create analytic models of different parts of the infrastructure to see how changes in hardware, applications or users will affect performance levels.

DISCIPLINE: Performance Capacity Management Tools

Discipline Roadmap for: Performance Capacity Management Tools

- **Discipline Boundaries:**
  - SNMP based software tools providing current and historical information that indicates how well a device or service is performing and has the ability to set acceptable thresholds based on the performance information.
  - **Capacity/Performance Management** tracks and manages the resources being used to satisfy the needs of the enterprise. These include storage capacity, disk space, CPU capacity, and personnel. The process also includes the creation and maintenance of a Capacity Plan.
- **Discipline Standards:**
  - All tools should support the implementation of ITIL best practices for service delivery and support.
- **Migration Considerations:**
  - A basic knowledge of ITIL best practices will be required.
- **Exception Considerations:**
  - Specialized Applications
- **Miscellaneous Notes:**
  - Forrester Research Inc. in Cambridge, Mass., states that no matter how sophisticated the analytics in the tools, the user still needs to have a thorough understanding of what parameters to model and then must interpret the data and ensure that it makes sense**.**
- **Established Date:**
  - November 2004
- **Date Last Updated:**
  - October 25, 2006
- **Next Review Date:**
  - October 2007

DISCIPLINE: Network/Events Monitoring

Discipline Roadmap for: Network/Events Monitoring

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Due to the length of the list of products in the baseline, the baseline is available on the final slide.	SNMP (refer to Security Domain for version) → The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for IT Service Support that addresses network events and monitoring. www.itil.com	Market Watch Market watch of ITIL and best practices for network events and monitoring.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

SNMP

Containment Targets

Other products in the baseline.

Emerging Platforms

Implications and Dependencies

Network monitoring tools are dependent upon the level of successful network device management and a detailed understanding of the relationships between network components.

Roadmap Notes

Standards must support state architecture’s recommendations for LAN topologies and WAN/LAN protocols. Gartner lists the following vendors as Market Leaders: ArcSight, CA, Novell, Intellitactics, NetIQ, netForensics and IBM

DISCIPLINE: Network/Events Monitoring

Discipline Roadmap for: Network/Events Monitoring

- **Discipline Boundaries:**
  - The requirement to ascertain network problems in near real-time to ensure maximum uptime, troubleshoot problems before they impact an agency's ability to conduct business and examine historical trends for capacity planning.
- **Discipline Minimum Standards:**
  - Monitoring tools should ensure that data can be collected and analyzed from all devices on the network. Additionally, the need to accommodate SNMP, syslogs, and other similar data or means of data collections to develop historical and actual trends. All end user support tools should aid the organization in adhering to ITIL best practices for Service Delivery and Support.

Migration Considerations:

  - As with adaptation of any new business practices, training will be required on best practices and systems or applications that are new to the organization. A basic knowledge of ITIL will be required.
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - April 27, 2005
- **Date Last Updated:**
  - October 25, 2006
- **Next Review Date:**
  - October 2007

DISCIPLINE: Network/Events Monitoring Tools

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current Baseline Environment

ACS
CiscoWorks
Envision (Analysis SW)
LAN scan
NetBotz
NetVision (Management Tools)
SMP (MRTG)
SNMP access to servers - OS tools to monitor
ELM Performance Manager 3.0
DS Expert 3.40
DS Analyzer v2.02
NetScan Pro 6.1
Microsoft MOM
IPMonitor

Cetus Storm Windows
IBM Director
MRTG
Cisco WAN Mgr
Nortel Optivity
SNMP Utilities
Watchguard Technologies
Bindview RMS 7.2
Whats Up Gold (7.4)
HP Openview
Somix WebNM
netForensics
Fluke Optiview
Cisco MARS

DISCIPLINE: Software Distribution Tools

Discipline Roadmap for: Software Distribution Tools

DOMAIN: PRESENTATION SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Novell Zenworks (SW Distribution) → SMS → SUS → Update Expert	The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for deploying software distribution tools. www.itil.com	Market watch of ITIL and best practices for software distribution.

Shared	Agency
	✓

Retirement Targets
N/A

Mainstream Platforms (must be supported)
Microsoft Systems Management Server (SMS), Novell Zenworks, SUS

Containment Targets
Update Expert. This product is restricted to patch management and not global software distribution.

Emerging Platforms
Market Watch

Implications and Dependencies
Each agency's selection of software distribution tools will be dependant on the Network Operating System(NOS) that is deployed. We have addressed the needs of Novell and Microsoft NOS.

Roadmap Notes:
According to Gartner (Desktop Management Best Practices), organizations are raising the bar in terms of what they want a software distribution solution to be able to address. Companies should search for complete life cycle management suites that include imaging, software distribution, patch, usage, user data and setting migration.

DISCIPLINE: Software Distribution Tools

Discipline Roadmap for: Software Distribution Tools

- **Discipline Boundaries:**
  - ❑ Policy: Policy and standardization are paramount to implementing a software distribution system. An example of a policy is restricting what users can download on their workstation computers.
  - ❑ People: One of the most-critical elements of a successful desktop management strategy is staffing. The best practice is to dedicate well-trained people to managing desktops. Even if you have resources dedicated, if they do not have sufficient training on the selected desktop configuration tool success will be limited.
  - ❑ Processes: Desktop configuration management processes must be defined to map to the life cycle of the PC and should include the following:
    - – Initial deployment along with the development of what should be included on each initial deployment.
    - – What should be included in system migrations
    - – When and how often system inventories should be done
    - – When and what needs to be packaged and tested before distribution
    - – When and how often software updates (including patching) should be done
    - – How troubleshooting and PC repair occur (for example, how long before re-imaging)
    - – Moves, adds and changes, as well as incident, problem, asset and configuration management
    - – Processes: Desktop configuration
- **Discipline Standards:**
  - ❑ All tools should support the implementation of ITIL best practices for service delivery and support.
- **Migration Considerations:**
  - ❑ Training should be implemented to ensure desktop configuration tool success.
  - ❑ A basic knowledge of ITIL is required.
- **Miscellaneous Notes:**
  - ❑ Survey in 2006 shows SMS and Zenworks still widely used. There is also the addition of Patch Manager/Patch Link for updates on Novell systems and it runs under Windows, too.
- **Established Date:**
  - ❑ July 28, 2004
- **Date Last Updated:**
  - ❑ October 25, 2006
- **Next Review Date:**
  - ❑ October 2007

DISCIPLINE: End User Support Tools

Discipline Roadmap for: End User Support Tools (Help/Service Desk)

DOMAIN: SYSTEM MANAGEMENT SERVICES

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Intuit (BlueOcean) Track-IT UniPress FootPrints Epicor Clientele Front Range HEAT BMC Remedy	**Minimum requirements:** The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for deploying end user support tools. www.itil.com	Market watch of ITIL and best practices for end user support.

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)
Minimum requirements: Incident management; Change management; Service level management; Remote control; Open API; Web interface; Dashboard; Escalation; Ease of use; SQL database.

Containment Targets

Intuit (BlueOcean) Track-IT – no API's

Emerging Platforms

Market Watch

Implications and Dependencies
Recommend knowledgebase(s) to minimize problem resolution time and effort. Recommend self-service capability.

* Most important metrics - associated with customer satisfaction (# tickets per agent or other technical efficiency measures)

Roadmap Notes
Minimum standard to be reviewed annually after adoption by AOC. Gartner recognizes CA and BMC software as leaders and innovators in IT service desk solutions.

DISCIPLINE: End User Support Tools

Discipline Roadmap for: End User Support Tools (Help/Service Desk)

- **Discipline Boundaries:**
  - End User Support Tools should ensure that end users are receiving the appropriate assistance. This includes the responsibility of managing all procedures related to the identification, prioritization, and resolution of end user help requests, including the monitoring, tracking, and coordination of Help/Service Desk functions. The Help Desk Manager will also contribute to problem resolution by giving in-person, hands-on support to end users at the desktop level.
- **Minimum Standards:**
  - All end user support tools should aid the organization in adhering to ITIL best practices for Service Delivery and Support.

Migration Considerations:

  - Dependent on the product that data is being migrated to/from. If an API does not exist, migration could be costly.
  - A basic knowledge of ITIL will be required. Foundation training is recommended.
- **Exception Considerations:**
  - None
- **Miscellaneous Notes:**
  - None
- **Established Date**
  - September 22, 2004
- **Date Last Updated:**
  - October 25, 2006
- **Next Review Date:**
  - October 2007

Disaster Recovery Best Practices

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Preface

As the field of disaster recovery evolves and new expertise comes into being, new technologies and methodologies will reshape recovery strategies. Disaster Recovery Best Practices is intended to be an evolving reference and a compilation of contributions from many state agencies.

Your input on this reference is welcome. To contribute material or for questions and assistance, please contact:

Dietra Thomas
Business Continuity Coordinator
Division of the State CIO
4430 Broad River Road
Columbia, SC 29210-4012
(803) 896-0177
djt@cio.sc.gov

Disaster Recovery Best Practices

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Table of Contents

Page
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disaster Recovery Best Practices

Introduction

“Disaster Recovery” addresses that portion of a Business Continuity Plan which deals with the recovery of IT processing capabilities.

The measures and procedures put in place to provide disaster recovery are specific to:

E The criticality of each processing system and its assigned RTO (Recovery Time Objective).

E The tolerable data loss potential for that system and its assigned RPO (Recovery Point Objective).

E The hardware, software, networking and other operating environment characteristics of the system and its dependencies.

E The monetary and man-power resources of agencies.

E The recovery management preferences of agencies.

These factors constitute valid and varied differences between disaster recovery strategies and can result in wide discrepancies in the disaster recovery environments designed by different agencies. However, since common components share disaster recovery considerations, agencies are urged to share their techniques and experience.

Agencies are strongly urged to work together on their disaster recovery strategies, to pursue sharing backup and recovery facilities and resources, and to earnestly consider cooperative ventures.

Disaster Recovery Plans

<u>BEST PRACTICES</u>

✓ All IT facilities need documented Disaster Recovery plans.

✓ Copies of Disaster Recovery plans must be kept offsite and accessible to the recovery team.

✓ Disaster Recovery plans should be tested no less than once a year.

✓ Disaster Recovery plans must be maintained and should be reviewed for changes no less than once a year.

✓ Critical IT infrastructure requires Incident Response Plans (IRP), a type of Disaster Recovery plan specific to an infrastructure component, which specifies how to handle and recover from possible impacts that would impair that component's ability to deliver the necessary performance.

✓ Disaster Recovery plans must be supported by plans for all logistical support departments; such planning is contained in a Business Continuity Plan (BCP).

✓ Platforms which support distributed processing for one or more systems which require recovery should ideally plan for recovery at the same site. If different sites are chosen, then those sites should be sufficiently proximal to ensure the minimum throughput for each recovered system.

✓ If one or more related or co-dependent (front-end, back-end, etc.) IT facilities choose a given recovery site, then the other facilities sharing the co-dependency should consider choosing the same recovery site; co-dependent IT facilities should work jointly in developing their recovery strategies. Proximity not only reduces networking costs and transfer times but also reduces exposure to network disruption (fewer potential points) and recovery times.

Risk Assessment (RA)

A Risk Assessment identifies the threats to the business from natural or human-mediated (intentional or accidental) sources, rates the probability of the threats occurring, determines what impact each threat could have in consideration of the precautions and protections mounted against it, and produces a risk exposure factor for each threat, usually expressed as a probability of impact such as 1 in 10 chance of total loss, 5% probability of a power outage longer than 3 days, etc.

Risk exposures are primarily used to evaluate the degree to which a business should implement protection measures and how much investment is justified, especially for protecting structures which facilitate business processes such as buildings, power houses, network cables, communication towers, or other enabling facilities.

Risk Assessment data can be used in conjunction with the Business Impact Analysis to apply probabilities to business process outages. However, in terms of disaster recovery planning which deals with restoring IT business processes on which today's business environment is so highly dependent, it is generally accepted that IT has a zero risk exposure tolerance and so recovery planning is always required and the investment evaluation is based on the BIA alone (see "Business Impact Analysis").

BEST PRACTICES

- ✓ A RA should be conducted for all IT enabling facilities such as data center buildings, power houses, and external communications facilities (network cables, relay stations, towers, etc.)
- ✓ Based on its RA, appropriate protection and impact mitigation measures should be implemented for each IT enabling facility.
- ✓ RAs should be reviewed for changes no less than once a year.

Business Impact Analysis (BIA)

A Business Impact Analysis (BIA) identifies each processing system's criticality, i.e. how much impact would outage of the system cause, and how long after the outage occurs would the impact be incurred. Criticality is used to plan the recovery to acceptable recovery requirements, and to determine how much should be spent on recovery capabilities, considering the following caveats or Rules Of Thumb (ROT):

Rules **O**f **T**humb: (1) Technology can decrease recovery times & data loss exposure.
(2) The faster the recovery, the more costly the technology.

Impact can be both quantitative or qualitative. Quantitative impact is usually expressed in dollars, e.g. loss of income, fines, loss of business base, etc. Qualitative impact is usually expressed as a non-numeric description, e.g. loss of lives, disruption of emergency services, damage to business reputation, loss of trained employees, missed business opportunities, etc. Impact, whether quantitative or qualitative, must be correlated with how long after the outage the impact will be incurred. Some impacts occur once at a specified time after the outage and others have recurring, and sometimes varying, impacts at various times after the outage.

The combined impact / time lapse determines the criticality of the system as illustrated in the following chart showing **Gartner's Sample Classification:**

Recovery Class/Tier	Financial Impact	Legal or Contractual	Service Impact	System Name
Multisite application	$500,000 / day	No	Within 45 minutes	Order, Web
1	$200,000 / day	No	Within 24 hours	Order, Internal
1	$300,000 / day after 2 days	No	1 to 3 days	ERP
2	< $100,000	Yes	5 to 10 days	Finance Reporting
3	None	No	Not time-critical	Data Warehouse

Business Impact Analysis (BIA) continued

Recovery Class / Tier

Each recovery class (or tier) ranks the criticality of the system. The following basic criticality structure provides three criticality classes:

1 = HIGH: the system must be recovered within a **short time** or **significant harm or cost** will be incurred.

2 = MEDIUM: the system should be recovered within a **moderate time frame** or **some damage** will be incurred.

3 = LOW: **little or no damage** will be incurred for an **extended period of time**.

BEST PRACTICES

- ✓ All IT facilities need to conduct a BIA for all systems.
- ✓ BIAs are used to guide decisions on outage tolerance and how much to invest in reducing outage exposure.
- ✓ Based on these decisions, each system is assigned a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO).
- ✓ BIAs should be reviewed for changes no less than once a year.

Recovery Time Objective (RTO)

Recovery Time Objective (RTO) is the target lapse of time after a disaster by when the system should be recovered. In other words, RTO is the maximum amount of time which can elapse between the point in time when a disaster destroys the service and the point in time by which the service must be recovered or unacceptable consequences will ensue.

RTO sets a target limit on recovery time and hence is used to guide decisions in planning how recovery from a disaster will be achieved. Recovery options are limited by how much expenditure is justifiable to achieve recovery in a given time. Generally, the faster the recovery, the more expensive the solution.

Recovery investment is a business decision determined by weighing the costs of lengthening outage periods (see BIA) against the increasing expenditures needed to shorten the outage period. A realistic RTO is one which can be met by methods which fall within the recovery investment limit.

BEST PRACTICES

- ✓ RTOs are best indicated by a Business Impact Analysis.
- ✓ A realistic RTO is one that is achievable within expenditure limits.
- ✓ All systems should be assigned a RTO, even those with low criticality.

Recovery Point Objective (RPO)

Recovery Point Objective (RPO) is the target point of recovered work. This is the state of work which will be restored to the recovered system after a disaster. Work can only be restored to the point at which it was last saved and removed to safe-keeping before the disaster.

Potential data loss is calculated by adding the times between backups and the time lapse until the backup is stowed in a safe place. It is the sum of the time since the last backup was taken and when it is safely stowed offsite.

Consider, for example, the following scenario of a "weekly" backup:

- ↓ backup1 is taken on Friday, March 5
- ↓ backup1 tapes are packaged on Monday, March 8
- ↓ backup1 boxes are stowed in the offsite vault on Tuesday, March 9
- ↓ backup2 is taken Friday night, March 12
- ↓ backup2 tapes are packaged on Monday, March 15
- ↓ disaster destroys the data center at 03:05 am Tuesday, March 16
- ↓ the only backup available for restore is backup1, taken March 5 = **11 days previous**.

If the potential data loss is more than the desired RPO, then backup and storage procedures and timing should be adjusted accordingly. In general, the lower the RPO, the more expensive the solution to achieve it. Financial considerations can increase the tolerance for a higher RPO.

BEST PRACTICES

- ✓ The frequency of backup creation is guided by the Recovery Point Objective (RPO).
- ✓ The procedure to stow backups offsite is guided by the RPO.

Recovery Point Objective (RPO) continued

BEST PRACTICES continued

✓ Backups should be stored offsite in a location which is:

↓ Suitable for the physical protection of the media and its contents.

↓ Secure.

↓ Accessible by disaster recovery teams.

✓ To improve the probability of a readable copy, keep at least two full backups in offsite storage, in addition to the full backup being taken and shipped to offsite storage.

✓ To ensure data integrity, a media retention plan should be developed and formalized where tape media is tracked during its life cycle. Retention and re-use rates should be based on the media's reliability metrics including length of life and number of uses. The purpose of this plan is to insure that media is retired before data is lost.

Typical RTO’s and RPO’s

Gartner’s suggested **Business Process Service Levels:**

Class	**Business Process Services**	**Service Levels**				
		Scheduled Hrs x Days	Availability		RTO	RPO
			%	Downtime		
1 * (RTE)	o Customer-/ Partner-Facing o Functions Critical to Revenue Production	24 x 7	99.9 %	< 45 mins. / month	2 hrs.	0 hrs.
2	o Less-Critical Revenue-Producing Functions o Supply Chain	24 x 6 ¾	99.5 %	< 3.5 hrs. / month	8 – 24 hrs.	4 hrs.
3	o Enterprise Back-Office Functions	18 x 7	99 %	< 5.5 hrs. / month	3 days	1 day
4	o Departmental Functions	24 x 6 ½	98 %	< 13.5 hrs. / month	5 days	1 day

* Class 1 application services are those with a RTE (Real-Time Enterprise) strategy and are those that the enterprise would suffer irreparable harm from if they were unavailable.

Sample Procedure to Build a Disaster Recovery Plan

1. Perform a Risk Assessment (RA) to identify the risk exposures. See “Risk Assessment (RA)” for more information on RA.

2. Use the results of the RA to determine and implement requisite protection and precaution measures.

3. Identify every application and the IT resources required to support it.

4. Perform a Business Impact Analysis (BIA) to determine the quantitative and qualitative cost per unit of time of application outage for all the applications. See “Business Impact Analysis (BIA)” for more information on BIA.

5. Determine how much expenditure can be justified to mitigate the outage costs identified in the BIA.

6. Determine the Recovery Time Objective (RTO) for each application. See “Recovery Time Objective (RTO)” for more information on RTO.

7. Determine the Recovery Point Objective (RPO) for each application. See “Recovery Point Objective (RPO)” for more information on RPO.

8. Design (or review) a backup methodology for the application to ensure the RPO can be met. Storage vendors and storage services can present available options which include:

   a. Performing tape backups and transporting the tapes to an offsite vault.

   b. Managing your own offsite storage facility (vault) or contracting with a storage service provider.

   c. Performing backups directly to offsite tape.

   d. Using dasd mirrors to enable taking tape backups with no (or less) application downtime.

   e. Creating synchronous or asynchronous copies on offsite dasd.

Sample Procedure to Build a Disaster Recovery Plan continued

9. Design a recovery strategy for the application to ensure the RTO can be met. Recovery site providers and recovery service providers can present available options which include:

   a. **Hot Site** – a fully serviced facility providing the necessary environment (A/C, power, water, cabling facilities, etc.) provisioned with all required hardware which is loaded, configured and ready to go.

   b. **Warm Site** – same as a hot site but the software (OS/applications, etc) will need to be loaded and configured.

   c. **Cold Site** - a fully serviced facility providing the necessary environment (A/C, power, water, cabling facilities, etc.) which will need to be provisioned with the required hardware.

   d. **Mobile Site** – an IT facility which is delivered to a pre-determined recovery site and may, or may not, house the required hardware upon delivery.

   e. **Hot Drop** or **Quick Ship** – an arrangement with a provider to deliver a hardware component within a pre-arranged time much shorter than normal; these arrangements provide for priority to be given to these orders upon short notice and typically contain provisions to shorten or circumvent delays associated with the usual procurement process.

10. Document the Disaster Recovery Plan ensuring that (1) the plan will be accessible after a disaster, and (2) procedures are put in place to maintain the plan.

    Note: The plan will be more current and useable (and its maintenance easier and less frequent) if titles, positions or functions are used in the main body of the plan while citing specific names only in appendices and where the documentation is person-specific, such as contact lists.

    The plan documentation should include:

    a. Specific recovery procedures sufficiently detailed that they could be implemented by someone with the appropriate skill set but no knowledge of the agency or its functioning.

Sample Procedure to Build a Disaster Recovery Plan continued

10. b. An action plan detailing who is responsible for what and when, including:

- who assesses the situation and what criteria are used,
- who declares disaster and the procedures involved,
- who builds the recovery environment and the procedures involved,
- who comprises the recovery teams and who are the alternates,
- who activates the recovery teams and the notification procedures,
- who manages funding and other procurement needs,
- who manages the recovery process, resolves problems and conflicts, and makes management decisions, and
- what the reporting structure is, complete with contact numbers.

b. All support documentation including:

- Contracts and other legal documents.
- Graphical summaries (maps, charts, diagrams, etc.).
- Technical references, guides, procedures and other documentation.
- Reference information such as directories, inventories, indices, and other 'look-up' references.
- Pre-printed forms or other process defining tools.
- Contact information for

(1) recovery team members and recovery managers,

(2) employees and their emergency contacts (next of kin),

(3) normal providers, alternate providers, and providers of recovery services,

(4) hardware servicing and software support,

(5) customers and users,

(6) local, county, state and federal emergency services,

(7) governing bodies, related agencies and other stake holders.

Sample Procedure to Build a Disaster Recovery Plan continued

11. Design and implement procedures to test the plan and apply updates. It is desirable to have different people man the tests so that as many people as possible are familiar with the details of the plan and the recovery process; this improves the likelihood of having experience available for an actual recovery.

12. Design a method for detecting and applying changes to keep the plan current. This is critical to ensuring that the plan will be effective when it is needed; constant change is a business reality, for example, consider how frequently a business must update its telephone list.

13. The entire plan should be exercised no less than once a year; portions may be exercised independently more frequently, especially to verify modifications. This process checks for changes, verifies if expectations are still realistic, and provides the opportunity to train employees and reinforce plan knowledge.

14. Monitor business changes that could impact the plan. Organizational changes may impact departmental interfaces or affect the way logistical support is provided. A location on which the plan depends on may no longer provide the expected facility. Provider agreements may change procurement plans. It is important to remain mindful of the plan dependencies and watch for any changes affecting those dependencies which could adversely impact the plan.

Acknowledgements

AOC subcommittee, Systems Management Services, January – December 2004
Doug Mader, DOR (Chair) – End-User Support
Russell Collier, DHEC – Network Events Monitoring
Debbie Dunn, CIO – Asset Management
Lee Foster, DOT – Software Distribution
Dave Gerth, CIO – Problem/Change/Configuration Management
Eric Pinckney, CIO (CIO support group liaison)
Floyd Stayner, DNR – Network Events Monitoring
Dietra Thomas, CIO – Disaster Recovery
John Ward, DOC (AOC Coordinator)
Charlie Zeberlein, CIO - Performance and Capacity Management